eForensics Magazine

50+ Network

VOL. 2 NO. 2

DAMON PETRAGLIA OF CHARTSTONE CONSULTING

MASTER BOOT RECORD MALWARE ANALYSIS

INSIDER THREATS

CLOUD FORENSICS

McCann INVESTIGATIONS

Issue 22/2012 (1) August

CYBERDIN

YOUR CYBER DOMAIN INSPECTOR

CYBER AND SCADA SECURITY

CLICK HERE

DENIAL OF SERVICE SIMULATOR

CLICK HERE

CYBERDIN INTRUSION DETECTION

CLICK HERE

WEB APPLICATION PENETRATION

CLICK HERE

STATION HARDENING BYPASS

CLICK HERE

PRODUCT PENETRATION TESTS

CLICK HERE

ABOUT US

01 Cyberdin - Your Cyber Domain Inspector, is a leading cyber security and penetration services provider.

02 Specializes in cybercrime, application & network security and security products bypass.

03 Led by a senior team, former IDF intelligence and information security units (8200 unit).

OUR SERVICES

Cyberdin provides wide rang of service in the Cyber security and the Penetration testing area.

- Cyber & SCADA Security
- Denial of Service Simulator
- Web Application Penetration
- Station Hardening Bypass
- Product Penetration Tests
- Mobile Applications Penetration
- Cyberdin Intrusion Detection
- Wireless Penetration Test
- Biometric Systems Penetration

DENIAL OF SERVICE (DOS) SIMULATOR

Denial of Service Simulator

CyberDin developed unique and advanced Denial of Service (DOS) simulators and DDOS network architecture that allows simulate current and future DDOS and Application Layer DOS attacks...

eForensics Magazine

TEAM

Editor: Paulina Rdzanek
paulina.rdzanek@software.com.pl

Betatesters/Proofreaders: Gabriele Biondo, Derek Thomas, Francesco Consiglio, Danny Lavardera, Salvatore Fiorillo, Sean E., Olivie Caleff, Jeff Weaver, Sailaja Aduri, Matthew Harvey, David Shave, Nivolas Villatte, O Davies, Dyana Pearson.

Senior Consultant/Publisher: Paweł Marciniak

Editor-in-chief: Maciej Kożuszek
maciej.kozuszek@software.com.pl

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Mateusz Jagielski
mateuszjagielski@gmail.com

DTP: Mateusz Jagielski

Production Director: *Andrzej Kuca*
andrzej.kuca@software.com.pl

Marketing Director: Ewa Dudzic

Publisher: Software Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.eforensicsmag.com

Dear eForensics Readers!

Today's the day! The issue of eForensics Magazine is finally available! The technology is constantly improving and our magazine helps the cyber security communities to develop their techinques in order to make our computers safe and secure in the industrial world. You will find hints and tips concerning not only Malware forensics but also many more cyber security themes.

In the issue you will find an interview with Damon Petraglia conducted by Liora Farkovitz titled "A Journey into the Mind: How the use of Psychological Analysis Techniques give Computer Forensics Investigators Insight into How Criminals Hide Evidence on Computer and Networks". Thanks to the fact that Damon Petraglia combined his Bachelors in Psychology with an advanced computer forensics degree, he uses both technical and psychological savvvy to gain access to sensitive data. Apart form interview, you will find Petraglia's article "Insider Threats".

In the malware section, you will find Patrick Olsen and BJ Gleason's article that provides information about Virtual Machines and MBR Malware. The authors give advice how to unpack malware, how to modify binary executables and how to analyse MBR Malware. What is more, Jan Gobel's "A Short Introduction to Malware Analysis" presents a short guide on how to get an overview of a malware's functionality through static analysis. He also briefly shows how the usage of IDA scripts can facilitate the analysis process by presenting a deobfuscation routine to reveal obfuscated strings of an example binary.

Next, in his article "Computer Forensics in China Final" computer forensics pioneer Erik Laykin shares some of his experiences and observations regarding the hurdles often faced when managing electronic data collections in this dynamic and emerging market. Also, Roman Gorban shows how you will learn about certain areas of Russian data protection legislation. You will learn about approaches commonly used in Russia to collect electronic evidence. Nevertheless, the magazine is not solely devoted to forensics. Ahahrzad Zargari and David Benford's article "Cloud Forensics as a New Technology" provides an overview of cloud forensics including the issues and the existing challenges in order to give better future prospects and offers some steps to be taken to overcome these challenges.

Evidence handling is considered one of the most important aspects in the entire forensic investigation process, as it is the first interaction between the Forensic Analyst and the evidence. Do you find it interesting? Elias Psyllos wrote two articles devoted to the topic "Evidence Handling for Mobile Devices" as well as "Evidence Handling for Digital Media".

Have you ever thought how we can ensure that we have the correct settings in place and how we can get the most secure connection? You will find the answer to this question in Paul Gafa's article titled "How Secure Is My Remote Connection?"

In the final section, you will find an extra article about CCTO written by Mark Sugrue. It provides you with the information on how to learn about CCTV industry and 3rd party player applications.

I hope that you will find this issue worthwhile. If you have any suggestions concerning topics, problems you want to read about or people you would like to know better thanks to eForensics Magazine. Please, feel free to contact us at www.eforensicsmag.com

Thank you all for your great support and invaluable help.

Enjoy reading!
Paulina Rdzanek

INTERVIEW

6. A JOURNEY INTO THE MIND: HOW THE USE OF PSYCHOLOGICAL ANALYSIS TECHNIQUES GIVE COMPUTER FORENSICS INVESTIGATORS INSIGHT INTO HOW CRIMINALS HIDE EVIDENCE ON COMPUTER AND NETWORKS

Interview with DAMON PETRAGLIA

I really enjoyed working with the criminal population. I started to become interested in criminology and the criminal justice field. 9/11 was a turning point for me. When that happened I decided I was going to go back to school because I had some direct involvement in the aftermath of the 9/11 attacks. That's a pretty life-changing experience "
In the interview Damon Petraglia discusses how to, in both technical and psychological savvy, gain access to sensitive data.

INSIDER THREATS

14. INSIDER THREATS

by DAMON PETRAGLIA

Insiders have the trust, confidentiality and access to execute attacks. An inside attacker will have a higher probability of success in infiltration or modification of critical information than any other attacker. The insider also represents the greatest challenge to securing sensitive data because they retain a privileged or authorized a level of access and are granted a certain degree of trust.
In his article Damon Petraglia shows how to detect an insider attackers as well as he gives a human behavioral indicators that help to notice them.

EVIDENCE HANDLING

16. EVIDENCE HANDLING FOR MOBILE DEVICES

by ELIAS PSYLLOS

Mobile devices are becoming more prevalent as evidence, in cases and investigations, whether it is for corporate or law enforcement. Mobile devices play a huge role in our everyday lives, so, the amount of data that passes through them can be extremely important for a case."
In his article, Elias Psyllos gives tips to consider when handling Mobile Devices.

20. EVIDENCE HANDLING FOR DIGITAL MEDIA

by ELIAS PSYLLOS

When entering a situation that will involve handling of digital media, the first step should be to photograph the location in which the potential evidence is located. Photographs show a 360-degree view of the location, prior to taking any action. This allows the analyst to depict the location as found upon arrival. The second step involved with evidence handling would be to photograph the digital media in question.
Elias Psyllos presents tips to consider when handling Digital Media.

MALWARE ANALYSIS

24. A SHORT INTRODUCTION TO MALWARE ANALYSIS

by JAN GOBEL

Malware has become an almost tolerated threat of the Internet. Private hosts and enterprise clients get compromised every day and the number of files to analyse is growing constantly. Automated sandbox systems have evolved to counter this threat, but they are not always the solution of all problems. Thus, knowing how to manually investigate a malicious binary and obtain the most important information must not be forgotten.
Jan Gobel presents some tips how to briefly analyze a malicious binary in order to get an overview of its main functionality as well as network indicators to be able to detect other infected systems on the network.

28. MASTER BOOT RECORD MALWARE ANALYSIS

by PATRICK OLSEN, BJ GLEASON

Master Boot Record (MBR) malware is making a return. Once confined to floppy disks, the technique is now being used to install botnet-based rootkits. In this article, we will show the basics of how MBR malware is deployed, how it installs itself, and how you can start to analyze what it is and what it is doing.
I their article Patrick Olsen and BJ Gleason give advices how to unpack malware, modify binary executables and analyze MBR malware.

FORENSICS IN THE WORLD

CLOUD FORENSICS

SECURITY

EXTRAS

A JOURNEY INTO THE MIND

How the use of Psychological Analysis Techniques give Computer Forensics Investigators Insight into How Criminals Hide Evidence on Computers and Networks

By Liora Farkovitz

This week was the 11th anniversary of the Al Qaeda Terrorist Attacks here in New York. On Tuesday of this week, this was the same day of the week of the attacks; the weather was identical with an incredibly clear and shiny sky. It was a warm and beautiful day, which with those traumatic memories well installed in the minds and bodies of my fellow New Yorkers, was actually a bit unnerving. We came through the Battery Tunnel with my heart rate rising and my husbands anxiety rising as well, and we momentarily bickered about whether the West Side Highway was open or blocked off. The memorial ceremonies had just begun and we were within minutes of the ‚moment of silence' which made traffic up and down the FDR on the east side, and all around Lower Manhattan totally insane. While we slugged through traffic towards the Upper East Side, we found precinct after precinct barricaded by crusty and intense police officers, who seemed a little more strident and insistent than usual. By the time I got to my appointment, everyone was raw with emotion, traumatic memories - short on patience and brittle with pain.

Personally, I did not live in New York at the time of the attacks; I had just given birth to my youngest child a few months before, and days before flown across the country in the same type of jet used as missiles in lower Manhattan. But no matter where you were that day, for all of us it was a seminal moment – I will never forget quickly calculating 110 floors x 2 x 250 people per floor as the number of potential victims while I waited for my four year old daughter to be released from her school and into my terrified arms.

It was the day that everything changed in America, and for every American – and the changes continue to reverberate today as our government pursues the enemies that were first identified through "intense internet chatter" using technology and stealth techniques alike.

Coincidentally, that was the same day that the subject of my interview, Damon Petraglia, changed the course of his career, and his life, when he decided to combine his Bachelors in Psychology with an advanced computer forensics degree. He declines to publicly share the particular details of that day in respect of the victims and their families but the story of how he developed his expertise from that day forward is fascinating indeed.

I interviewed Damon Petraglia of Chartstone Consulting, a Digital Forensic and Information Security consulting company located in the state of Connecticut, not very far from New York, New York. Damon is a computer forensic expert. He teaches information security to US federal agencies, holds a master's degree in forensic computer investigation, and has lead security assessments and breach investigations for both public and private sector clients throughout the country and internationally. Additionally, he teaches law enforcement and is a member of the electronic crimes task force for the US Secret Service.

Mr. Petraglia took me on an amazing journey through the minds of the people that are charged to protect our systems, criminals, and himself as an Investigator - and how he uses both technical and psychological savvy to gain access to sensitive data.

LF: Tell me about how you got started in this business and what you enjoy doing. What's unique about your practice that might be different than others…this interview series seems to be turning more into talking to different consultants about how they apply this skill set within the commercial sector?

The first interview I did from a law enforcement angle, and I talked to someone this morning who also owns a consultancy and I have a couple of other interviews with people who own consultancies too. So that should be a different way of approaching this from what I did before.

DP: Well, I thought the one with Shaun Winter was absolutely fantastic. I really like that.

LF: Oh thanks! Let's start from the beginning of the story. How did you get here, and what are your areas of specialty? Why do you like what you're doing? The magazine always wants to know, what is it that you would advise somebody who wanted to do what you're doing in their careers?

I think that they like that angle because they're appealing to a younger audience and we get to be considered, what's the term I want to use? Seasoned.

DP: Right (and you can hear his smile).

LF: Maybe stories that you have of that. If you want to share stories about things you've done for law enforcement and things you've done for corporations or things that you may have done for individuals, anything that's been international because this is an internationally based magazine.

Let's just start with when you started out in your career, what was your career? I'm 50, so when I started in technology, I had the background of social work degree and I thought that I would end up being a marriage therapist, honestly. That's where I thought I'd end up, and I ended up in technology for many years. So I kind of bring a fusion to that and I find that other people that are in my age group do too.

DP: Yeah. Actually, I think you and I have more in common than we may realize. I'm a little bit younger. I'm 41. I started out with a bachelor's degree in psychology, and I started out working with troubled youth, we'll call them. So basically it was a reform school or even a sort of correctional facility for youth, and from there I actually jumped out and went into sales because of the money. But I really enjoyed working with the criminal population. I started to become interested in criminology and the criminal justice field. 9/11 was a turning point for me. When that happened I decided I was going to go back to school because I had some direct involvement in the aftermath of the 9/11 attacks. That's a pretty life-changing experience and I decided I'm going to go back to school. I need to help people. That's what I've always wanted to do all my life, and this is something that I'm going to dedicate my life to.

LF: I think that many of us experienced a great deal of intensity and introspection as a result of the terrorist attack and it changed all of us, I mean, I can remember that day. I married an artist who's from New York and that's how I ended up in Brooklyn. I know you can tell from my voice that I'm not from here, but I moved here from Atlanta, and at the time of the World Trade Center attacks I was married to my first husband and my third child had just been born a couple of months before and I'll never forget it.
It changed everything the way I thought about everything, and my husband, he's told me stories that at the time, he was on Lafayette in Manhattan. He could see what was going on from the roof of his building. There was debris in the streets, people posting for information about loved ones near where he lived at the time. He can't watch any of these shows that come on TV. I can pretty much watch anything that's forensic that comes on, but he just can't. He can't do it. It's too upsetting to him.

A lot of my own work has been about how trauma affects us as people and how that's played out. A lot of the projects I've done research for were how to treat trauma remotely using telemedical solutions, how to create reports showing the effects of trauma, or how to document the medical records for trauma treatment, so this is a big part of the kinds of research and development projects I've done, and I certainly do understand the affect of it. One of the things I did last year was I became a Disability Advocate for the courts. In the courtroom it's so stressful that a lot of people just can't articulate themselves.

So when you went back to school, where did you go? Did

you go there in Connecticut or did you come here to the city?

DP: No, I came back to Connecticut and immediately said, „I want to do something bigger and help people." First thoughts were things like the FBI and that kind of thing, you know? What do I have to do, and where do I need to go?

At the University of New Haven they have an excellent criminal justice program and so I went there and asked to speak to the head of forensics and said, „Here I am. I'm 30 years old. I'm not a kid so let me in. I want to pursue a master's degree in forensics," and he said, „No, you don't have enough hard science background." So being 30 years old and realizing sometimes you don't always take „no" for an answer, and so I kind of said, „Well, who's your boss? I want to talk to him." I went and talked to the Dean of the entire Criminal Justice Program, which forensics was a part of, and the Dean said, „Well, if the forensics department isn't going to let you in, I like what I see. I understand where you're coming from. What do you think of this? We have this new program. It's called Computer Forensics." At the time I didn't own a computer.

LF: Wow!!

DP: And I did well.

LF: That is just amazing that you didn't have a computer then.

DP: Yeah, I didn't. I mean, it was 2002. I wasn't working a job where I needed a computer. I didn't have one. I used a couple here and there, so I said, „Well, this is interesting because everybody's going to be using a computer soon and just because I'm not, I'm a little bit behind things." I immediately saw that it was possible that every crime was going to have some evidence back to a computer, and I could see that pretty quickly, so I said, „Yes, if you let me in this program I'll do great." So he let me in, and I did. I did really great. I graduated with a 3.8 or a 3.9, and did very well. During that program I became a graduate assistant in that department and I assisted in teaching some of the computer forensic classes and then was invited to teach a course in computer forensics at the police academy in Puerto Rico. So I did that and I graduated the program and immediately became a contracted federal investigator for The Office or Personnel Management (OPM). And what I did was background investigations for security clearances. So people that needed top secret clearances to work in government projects, I would do their background.

LF: Did you find anything surprising in doing that work, things that people were trying to hide?

DP: Oh, yeah. What had happened was, I was very good at investigations and I quite quickly was put on what they call Special Investigations and pretty soon my entire caseload was foreign names that were impossible to pronounce.

LF: Names like Liora Farkovitz perhaps? (laughing)

DP: Much tougher than that. So the work was very, very interesting because I was dealing with international persons and situations. I got to see a lot of things. I got to see the inside of many submarines, doing some military investigations, and got to meet and incredible amount of people and an incredible diversity of people. So it was really interesting work and so then while I was doing that I wound up doing an investigation and being offered a job with a consulting company and wound up doing information security consulting. They hired me because I had the master's degree in forensics and they were trying to get a forensic program off the ground. I said, „Hire me and we'll take it from there." From there, I travelled all over the country on all kinds of different information security projects from penetration testing, being the hacker, to policy and procedure reviews to physical penetration and a lot of Social Engineering projects. Are you familiar with Social Engineering?

LF: This is one of the things when I was looking into what you were saying yesterday that I don't know what that means. This could be the highlight of what I write about with you because I know what Social Engineering is from a social sciences perspective or from a policy perspective but not in the context that you seem to be going towards, so, no. I don't know what Social Engineering is and I'm very curious.

DP: I think the easiest way to kind of describe it and maybe for your readers, they would understand it as being the "con man" or manipulating another person and what I always kind of tell people is, "You know what a computer hacker is... well instead of hacking a computer, I hack people!"

It's just manipulating that person into giving me sensitive information, and sometimes this is quite a long process involving quite a few people because it's not that easy to just walk up to someone and say, „Hey, give me your username and password." You may have to ask them very simple questions like, „What's your name?" and then use that person, „Oh, hey, I was just talking to Joe Smith." Well the next person that hears you talked to Joe Smith, they know Joe Smith. They feel a little bit comfortable with you because they think now you have a connection. Now you talk to that person, „Well, since I was talking to Joe Smith, he told me to come talk to you and you might know the phone number of," whoever it is, „the supervisor." They may be more apt to give you that phone number. So each time you leverage a little bit more. So that's really what Social Engineering is.

LF: Towards what end would you be using those skill sets in your work though?

DP: OK. So one of the things I've done and continue to do is the Social Engineering test, and this tests the security of any particular environment. If you have a network and you've got sensitive information on that network, you want to do certain things like penetration testing. You want to make sure that's not vulnerable to hackers. Well, part of securing a network or securing your facility or whatever, is making sure your people aren't vulnerable either. So you harden your network, but you got to harden your people too and make them understand...

LF: That's interesting because people aren't talking about the human aspect of security in the same way that they used to. This is the first time I've heard about this in ages.

DP: So far I've been 100 percent successful in acquiring every target I've desired using Social Engineering, so it works every time if you know how to do it. Part of knowing how to do it, you have got to understand people. I understand psychology so I understand human nature. I was a trained investigator so I can size someone up and recognize what makes them tick very quickly so I can choose the best approach. Sometimes

the best approach is to be authoritative and force a person into do something or tell them, „Give me this information," because they'll crumble and do it quickly. Other people don't like that and you have to schmooze them a little more and be very polite, and most of the time the thing that works the best is when they feel like they're helping you. So you just have to know what to use and when to use it and the thing is that I have used this on incredibly secure and very sophisticated networks where the test was three or four guys next to me trying to hack into the network, getting nowhere and me picking up the phone, calling their help desk and within a few minutes I've got the administrative rights to the entire network just by discussing it with somebody. Again, you're using and leveraging information from previous phone calls or other things that you might know about.

LF: So let's take that a step further. So once you've been able to gain the trust of your target, if you will, what happens then? You go back to the organization and you say, „These are the ways in which you're vulnerable?"

DP: Yeah, exactly. What normally I would do is, and let me make sure your readers understand, you have to be authorized to do this, otherwise…

LF: Yeah, it's not kosher to do on your own.

DP: Yeah. Don't just go try it. It's a „don't try this at home" kind of thing. No, you have to be authorized. So, number one, I've got a letter of authorization with me because if they do call the police or if your physically doing this, because I've broken into very high security facilities by talking my way right in, telling them I'm somebody that I'm not. I've posed as a new employee. I mean, I could tell you stories that would probably have you laughing and then also going, „Oh, my god. I can't believe somebody fell for this stuff." You know, it's kind of scary. So, you have to be authorized to do it and then you, if you're the consultant, will work with the client to select the targets and the client probably will have a target in mind like, „Can you get into our data center?" or „Can you get these specific administrative credentials?" So once you get those, there's a couple of different ways you can go about it. Basically, once you've acquired your target you can then go further and see what their response is and assess their response to an incident so, basically get yourself caught and make it known you're doing something at that point and see what they do and see what they're response is and then you can assess them and assist them on how to respond to incidents, or, most of the time, I would just slip out undetected. I would get what I wanted, say 'thank you very much', walk away without every being confronted and they have no idea that I've stolen their crown jewels.

LF: Wow!!

DP: Then you go back. You call your point of contact with your client and say, „Hey, look. This is what happened. I acquired the target. I got what I wanted. So we've been able to breach it and if you haven't been notified by your own people that something was going on then we've got a serious problem." So then you kind of break down what happened, who you spoke to, how you did it, and you find, „OK, here's where the vulnerabilities in the processes, the procedures, the policies, and the human beings…why did they not recognize it? What level of training have they received and why didn't they recognize that they shouldn't have been giving me the information they did?"

LF: So does that result in their doing a knee-jerk reaction in firing people?

DP: No.

LF: Or do they decide it's matter of their lack of training or policies that are weak?

DP: Yeah, that's really what it is. That's one thing I always kind of go into this when we're setting up the statement of work and really defining the scope of this, is that your people should not be fired. This shouldn't be some kind of witch hunt where you're going to get people in trouble because, Mr. Company -Owner, this really is your fault because you didn't train your people well enough. You didn't supply or give them the necessary resources and training.

LF: Or you didn't know what you were doing, right?

DP: Yeah, so when they feel like it's their responsibility, they're much less likely to go firing people. My thing is, I want to go into a place and I want to increase your security posture, and just going in and firing people, that's not going to do anything to help you.

LF: No, blaming wouldn't.

DP: Yeah, so let's figure out where your vulnerabilities are and let's fix them, and that's the key.

LF: One of things I was just curious, just kind of winding back around to the kinds of things that you were interested in younger, was this the sort of thing that when you were a kid that you liked to be able to do in sort of an espionage way to be able to see what you could accomplish in this sort of stealth manner? Or is this just something that you realized…how was it that you were able to identify this specialty? How is it that you realized that this was something that had this kind of a value to a company or to an organization?

DP: Well I think growing up, definitely I realized that I had the ability, especially with my parents, to get my way and get what I wanted by manipulating my parents without letting them know that they were being manipulated. I mean, to be honest with you, we all have that ability and we all use it from the time we're born.

LF: Sure.

DP: The crying child gets their way so often.

LF: Or they get it by smiling, so however that is…it's Pavlov.

DP: Exactly. So it's sort of an innate thing and then as I studied criminals and psychology and I really loved the abnormal psychology. I loved people that did things differently or thought differently. Not that I loved the serial killers, but I always just found those kind of…how is that person's brain wired? Why are they so different? Because I can't do that. But there were so many things that those people would do to manipulate their targets without their target knowing that they were being manipulated that I found absolutely fascinating. These are things that you can use for good or you can use for bad. So I don't know really where it started so much, but I think once I star-

ted learning about it and I realized, „OK, I'm in this forensic computer investigation program. I only just bought a computer when I joined the program. I'm not the most technical person, but I'm going to catch up and understand what these bad guys do so I can catch the bad guys." Well I started going more towards not the technology but the criminal themselves. Who are these hackers? Who are these computer criminals? Why do pedophiles do what they do on a computer? How do they do it on a computer?

LF: Right.

DP: What are these people doing? So I was always more intrigued by the psychology and human factor than I was by the technology. I mean, don't get me wrong, I'm fascinated by technology too.

LF: No, I understand. To me the computer is…people used to say, „Well how in the world could you end up working with technology when you have a social work degree?" To me, the social work is just an amalgamation of sociology, psychology, and anthropology.

DP: Right.

LF: How are those disciplines applied? It's a pragmatic application of those soft sciences. So people would ask me, „Well, how in the world could you ever be interested in technology?" It's the problem solving.

You have deductive reasoning. You have a set of variables. You're applying all the different ways that those variables can be applied, whether it is to the problem of the person that's using the computer as a tool or the tool itself because the truth of the matter is that the computer is modeled after how we function and store information and refer back to it. It's really not as sophisticated as our brain, but a lot of people think of it as being an extremely sophisticated device but when you compare the processing speed of a computer to the processing speed of the brain or the storage capacity of a computer hard drive to what we're able to store and to reference for almost a hundred years and the plasticity of our brain, there are many commonalities. I think that that's lost on a lot of people. You have a fascinating approach to what you do in your work and completely unexpected for me to find that.

DP: I haven't even talked about computer forensics yet!

LF: Well, forensics is computing and it's „How do you breach the network?" So if you're only looking at this from bits and bytes, obviously it isn't enough. You can beat your head against the wall for hours but if you can get in in 15 minutes because you're charming and good looking and you say the right thing then that's part of it.

DP: Yeah, absolutely. Forensics is really nothing more how the Law applies to a certain field coupled with general rules of evidence….so its not breaching the network as much as it is the investigative process to determine the who, what, where, when, why, how of the breach and the handling of the evidence for that particular case.

LF: That's part of the process as well and this is just when of your tools then.

DP: That's right.

LF: Once you breach the network using the Social Engineering technique, do they have a certain file they're asking you to look for or are they asking you to see if you can acquire credit card numbers or health care information or financial data that they're not telling you how to acquire? Or are they just going out there and saying, „What can you get ahold of?"

DP: I've got both ways. You know if you're at a financial company, their crown jewels are where that financial data is, and you know at a health care company, you know, the PHI or personally identifiable healthcare information. So if they say, „See what you can get," of course I kind of already know what the home run is going to be so that's what I'm going to focus on. But a lot of times they will say, „Look, we're doing research on the newest fuel cell and we want to make sure that that stuff's protected. Can you find it? Can you get it?" You know, that kind of stuff, or, „Can you actually, physically, get into our data center and plug a machine in?" So I've done it both ways: See how far you can go, and can you get A, B, and, or C.

LF: OK. That's very interesting. I'm going to jump back over to the profiling because you said, "What is it about the kind of person that gives you access?" I imagine there's been some point in time that someone has knowingly given you access that they might've suspected they shouldn't.

What kind of personality are you running into? Are these people with resentments? Or are they people trying to right a wrong? Or what do you feel motivates people to reveal the information that they do?

DP: I think probably the number one is playing on a person's emotion, especially sympathy and the desire to help another person, and most of the time they don't feel like they're giving away a company secret or they're doing anything wrong. They feel like,' it's OK to do because I'm helping that person that is looking at me right now'. For instance, New York City, not long after 9/11, while I was going to New York City, I was thinking to myself, „There is no way that the security guards in this building are going to let me go upstairs. I'm never going to get past the lobby where the security guards are because it's still too fresh in their minds. This is New York. It's not going to happen." So when I walked in and there were the security guards, and there were several. I want to say about five of them. So I was significantly outnumbered and so what I did was I went in and said, „I'm a new employee," completely lied and said that I had never been on a train before and I had just come in on a train to Grand Central and I said, „I went to go to the bathroom," again at Grand Central, „and I put my bag down with my laptop and all my stuff for my first day at work here," and I'm getting very flustered, „and someone ran off with my bag. I can't believe this." I'm starting to well up. I'm starting to tear, and these guys say, „Oh, man. C'mon. Go on ahead. Human Resources is on the fourth floor …'" or whatever it was. „Go on up there. Let them know what happened." So they felt real bad for me.

LF: Wow!

DP: And they let me right in. Now, I sure didn't go to human resources on the fourth floor. However, now that I'm on the sixth floor, anybody that asked me who I was or, „Where are

you going?" „Oh, I'm trying to find human resources. Isn't this the fourth floor?" „No, two floors down." So you leverage that information so it's even people that caught you didn't realize that they caught you, and then from that point I actually was able to access an executive's office and spend a lot of time in that office stealing very sensitive information. All because the security guards felt bad. Now, they knew they were giving me access which was wrong for them to do.

LF: Wow, again.

DP: But they felt like they were helping somebody that needed help.

LF: So what happened when you left, because I would imagine that they should've been able to see you walking around the building on camera or that they might have, I mean, did they have any idea what you had done?

DP: I had actually got out of the building without being detected with all of my sensitive information, and so then I came back in, and there was a lot of confusion on their faces, like, „Wait a second, what's going on?" So I said, „You guys need to call my point of contact, blah, blah." The one guy that was kind of leading the bunch said, „Son of a -. Man, I felt really bad for you." It was funny in one way, but in another it was not, because a few of them got pretty mad because I scammed them.

So I made these guys look bad and that wasn't my intention.

My intention was to be the bad guy. This is exactly what a bad guy's going to do and this is how they do it. So they felt bad for me, and then they were mad because they felt bad for me and they shouldn't have. But none of them got „in trouble." I don't know if they had to go through further training or anything like that, but even if they didn't have to go through further training, that's a mistake they're not going to make again because the five of them were pretty embarrassed.

LF: I imagine that they would've been embarrassed. That's a good story that goes with your explanation of Social Engineering. Have you ever worked on anything that had to do with government corruption or tracking down trafficking or anything of that nature?

DP: Yes, and only as part of investigations. I got to figure out how much I can really speak about it. I can try to give you an overview of what those investigations kind of look like but without disclosing any specifics.

LF: What's your take on it? What do you think makes someone like that tick?

DP: Well, I think there's a couple of things that go one with these type of cases where it appears so obvious that this is happening to a child and nobody's doing anything about it. There could be a number of reasons. The first and most obvious and hopefully the least frequent is just negligence on the part of people that it's reported to, and there's not much you can do about that. Some people will do really good jobs at things and some people won't. So you can't really do too much about that but then sometimes things get reported and there's already an ongoing and active investigation and if that's the case sometimes the person that's reporting it may sort of be blown off, not because of any other reason. During an active investigation, the investigators want others to stay out of it as much as possible. The investigators are doing things to catch the bad guy and any involvement outside of that really can screw things up for the investigation. So sometimes you may be ignored because there's an active investigation, and when that happens it's very hard on the person reporting it because you feel like you're being ignored.

And it's also hard. You've got to understand, an Investigator's job is very, very difficult because if you have to ignore somebody that just told you this and you can't give them any peace of mind, that's tough for you as a human being. Because if you're an investigator, you want to help people, and shutting them out here is totally going against your own grain. So it's hard on both parties on that one. So I think those are probably the two main reasons that this happens, or what happens, especially when you're at a large agency level, is that things do get lost. Caseloads become extremely large and when you have one investigator doing 100 cases, things are going to fall through the cracks. Unfortunately, that's a tough thing.

So there are a few different things. It could be negligence. It could be too large of a caseload. It could be an ongoing investigation. There's a lot of different reasons that something like that can happen, but the thing about that is that that's the kind of stuff you hear about and that's the kind of stuff that stays with you, but the truth is that most investigators, and I would say more than the majority of investigators, are going to do the right thing. So those kinds of things that you hear about are actually few and far between when you realize how many cases are being worked and how many cases are being resolved and how many children are being helped.

LF: Well, the ones that I see that are getting the most attention are the stranger attacks. Stranger attacks are being investigated but if they are family-based attacks, they're not being investigated in the same way. Law enforcement prosecutes strangers, but is required to involve the Administration of Children's Services when a family member is reported, so they are not empowered to investigate family members the way they do third party assaults. So that creates this big huge abyss where these cases fall through.

I was asked to look into a case once where, the Guardian ad Litem in that case has become a Superior Court Judge. The way that I became aware of her situation was that the mother was trying to get the Guardian ad Litem to properly investigate her allegations that her ex-husband was raping their son, and she had extensive medical evidence that he was being violated and there was also physical medical evidence and psychological evidence as well. One of the things that she said to me, and part of the reason I brought this up is because I need to get to the detail question that came up when I was talking to her about her case.
Her ex-husband had a job working in networking. He's a network administrator for a civic organization in their area. She told me that he had secured their home network in a very particular way - in a way that was almost a "signature" of his, in terms of his ability to secure a network.

Then she told me that when she had caught wind of this investigation that had been done involving the civic organization and how it was used to mask the use of their network for child pornography and child trafficking that she new he worked with - this was the "red flag" for her

personally which triggered her understanding of what he was doing to their son, and what he was capable of.

She began to suspect that he was involved in this kind of activity because the detail of how that network had been secured was identical to the way that hers had been secured in her home. One of the things that made me wonder, especially with your background in, I don't know if profiling is the appropriate term, but the psychology of this, do you see people develop a certain protocol or a certain signature for the way that they go about doing things or is there a set of standard ways in which a network is secured that is either right or wrong? Is there a wider variety way of ways to do this?

DP: I think your question is fantastic. I really like this question, but I kind of think it's a two part answer. Are there sort of signature ways that people do things on computers? Absolutely, and you see this very often with pedophiles or you see it very often with the way drug dealers will keep their files or who owes them money. So they keep their records in very particular ways. Pedophiles are very often, and I don't want to generalize, but very often they are incredibly well organized on the computer and will organize from their genre to alphabetizing exact folders for every little thing that they like about their crime, which is typically the pictures and video. So it'll be so incredibly organized that it's really unbelievable. So there are definitely sort of signature ways that certain criminals do certain things. Now that's going to be a little bit separate from how somebody secures their network. Now there are some things that you may be comfortable with and these security features may be employed regularly…

LF: But if somebody was hiding, I mean, this was from a perspective of, „OK, this guy, is incredibly detailed about his fetish, right?" Not to minimize what he's doing, but what he's doing is a fetish type of a behavior, but he wants to hide that. Then he's going to be extremely concerned that someone's going to identify this catalog of…it's basically documenting what I would say is a mental illness. He wants to hide that information so doesn't he go to particular extremes or an unusual way about hiding his crime?

DP: Well, it depends. Pedophiles that are living alone and things like that don't necessarily hide anything on their computers. A lot of times even their screen saver is something that would be considered illegal, so if they are married and living this „double life" or something like that, then sure. So it's certainly possible that you would prefer to encrypt files and I would prefer to use steganography, and so I might be really comfortable with steganography and that's how I hide my stuff. That may be what she was getting at as far as how he was securing things.

LF: What is steganography?

DP: Steganography is hiding a picture within another file. So you may have an illegal image of child exploitation and with a steganography program you can make that picture file a little bit bigger, the file size a little bit bigger, but it changes into a flower or a tree or something completely innocent looking and to open it you need the key to the steganography.

LF: Wow. I didn't have any idea that anything like that existed.

DP: Yeah, and they do have a lot of sophisticated programs and anybody that does child exploitation or is looking for things will run certain programs to search for known steganography programs or known steganography hash values and things like that.

LF: I know of a case that is part of a set of Inter-American Commission on Human Rights cases, where the Protective Mother has been trying to acquire evidence that the custodial father is distributing child pornography and she believes he has a special way of hiding it. I wonder if that is how he does it?

Part of the reason that I think that those cases in particular are so important is because there are many allegations that federal funding is being misused from non-profits that do not have enough oversight. The GAO announced that they don't know where 71% of this funding goes. This same woman was able to demonstrate that her ex-husband had been given more than $70,000 of government funds to pay for "more access" to their children through the state.

So there was a particular group of pedophiles who believe that what they're doing is normal, that they're just like gays, that they're so misunderstood and that adult-child sexual relationships are normal. So their agenda is to normalize the conduct and they infiltrated this system of funding and they provided ways to people in those circles to have access to legal resources and all kinds of things so that they could avoid capture. Many of them are trading pictures or access to children among themselves and because they're part of family units they're not really being investigated in quite the same way. So what you're describing would be a really good way of hiding that information and I would imagine that if you were looking for information to prove that that person was engaged in that kind of conduct, just even owning that software program would be a way of alerting your investigatory staff that there was something more to be found there because, what other kind of picture are you going to need to hide in that same way?

DP: Well, yeah. That's the thing. Depending on the type of case I might be working on, that's certainly something I'm going to look for. Now, a steganography program is not illegal to have. It's perfectly OK. However, depending on what that case is, that's going to raise a flag with me because are you trying to hide something simply…it could be as simple as a perfectly normal family unit but dad has some sexy pictures of mom that he doesn't want the kids to see. I got not problem with that.

LF: Yeah, I don't either.

DP: However, there's a big difference if this is a terrorist case and all of a sudden I find steganography programs. Why are those there? Why?

So if we don't have the sexy pictures of Mom, but all of a sudden we've got some bomb making plans, well then we've got some issues.

LF: Right, because then you want to know if they have converted documents to jpegs, because they can convert any image into a .jpeg and then hide it because it isn't only a photograph, it's a .jpeg image, right?

DP: Yeah, and there's so many different programs and there's things that you do with certain forensic programs called signature analysis because, you know, I can easily hide a .jpeg image by renaming it a .doc image and when the computer tries to open it it's going to say there's some kind of error and you're going to ignore it and not open it. However, if I do a signature analysis I can find all those ones where you altered the file extension or altered the signature in some way to figure out what those files really are.

LF: This has got to be another area that your interest in psychopathy and manipulation and the psychological motivation of someone and how they're going to function with that system is invaluable. Because you're not just sitting there going, you know, „What's the checksum of this file?" I mean, you're looking at, „How am I going to disguise my criminal behavior here?" It's a very interesting specialty. It's very, very interesting.

DP: Yeah. When you start looking, I mean, I've looked at hundreds of computers and when you start looking at a computer you are looking at that person's brain. It's unbelievable. I can tell you just about everything about a person by forensically looking at their computer and just poking around a little bit. I can tell you what kinds of, especially men's computers. I can almost certainly tell you if they're into blondes or if they're into brunettes and what body types. You know what I mean? Because you'll find a lot of those types of images, and the same thing with criminals. You kind of see how they organize things. You can see…it's really looking right into a person and I don't think you realize how much information is really on your own personal computer person.

LF: You really would. Damon, thank you so very much for your time with me today. I've learned so much, and I'm sure the eForensics Magazine readers will be equally fascinated.

What I found particularly fascinating about my interview with Damon is just how many different things that he does that have a technological foundation are so heavily affected by Psychological Analysis Techniques, and how Social Engineering is such a revealing technique. He's still searching and documenting and gaining technical access – but no matter how amazing the computers are that we have today, it would certainly seem that there our own "computational systems" are the most sophisticated tools we have to crack the forensic code.

Damon Petraglia is the director of a demanding forensic practice and core to the leadership of a highly visible security program. He performs forensic examination and investigation, vulnerability analysis and risk / threat assessment, social engineering testing, security architecture review, incident response, and policy and procedure review and development.

INSIDER THREATS

by Damon Petraglia, CRISC
Dir. of Forensic and Information Security Services

Insiders have the trust, confidentiality and access to execute attacks. An inside attacker will have a higher probability of success in exfiltration or modification of critical information than any other attacker. The insider also represents the greatest challenge to securing sensitive data because they retain a privileged or authorized a level of access and are granted a certain degree of trust.

Many times detection of an insider attack or breach is unintentional. Many detection activities lack focus as they are not an integrated part of a larger information security or risk management program. Commonly detection is initiated by things like a customer or end user who has noticed a problem. Many times auditors or coworkers will notice something suspicious. Unfortunately many times coworkers will not speak up simply because they do not have "proof" of wrong doing. Auditors or technical teams may notice or accidentally discover anomalies when system upgrades or routine maintenance are performed (this is when logging may become crucial and valuable evidence). Other notable indicators may include a sudden increase in competitive business and workers unable to perform their normal duties because they are devoting time to "other" activities.

There are human behavioral indicators which should be noted. Many of the following behaviors may or may NOT be indicators depending on the individual and their role within the organization. These behaviors should be recognized as anomalous or indicators when they deviate from the individual's normal day-to-day behaviors. Examples include:

- Taking critical, sensitive, proprietary data, trade secrets, and / or intellectual property home without a real or clear need for it, especially if it is not needed to complete their job duties.

- Remotely accessing the organization's network at odd times. Odd times would be "odd" to their normal behavior. If the individual logs on normally 2 to 3 times per week between 6pm and 9pm and all of a sudden they are logging on at 3am every day, that should be noted and investigated.

- Just as access at odd times, when an individual works odd times (times in which the majority of the workforce is NOT present), it may be an indicator that the individual wants to conceal what he or she is doing. Having less people around is desirable for this.

- A sudden peak in interest in business, processes, or materials outside the individual's normal scope of work and job duties. This could be that the individual wants more responsibility or wishes to expand or move within the organization; however when it is anomalous to the individual's normal baseline behavior it should be noted (especially if there is sudden interest in matters which relate to competitors or foreign countries).

- Increase in installing their own software or bypassing controls and policy regarding system, network and computer use.

- Changes in behavior such as increased paranoia, increased questioning about policy, increased questioning and interactions with co-workers on a personal level.

Different than human behavior anomalies are technical anomalies. Technical anomalies can be recognized by logging and correlation. This can be accomplished automatically or manually. The important things in using log monitoring are logging the correct things (e.g. access to sensitive files, attempted access to files, copying or movement of specific data, etc…), retention and review of logs, and well defined baselines to reduce false positive results. There are many tools for network monitoring which will alert for known malicious behavior and detect and report anomalous behavior. These should be used in conjunction with well-established policies and procedures and other technical tools such as data loss prevention tools.

Prevention comes with a blended response which includes operational and technical measures. At the fore front should be

an organization wide information security training and awareness program. The organization must train all employees that the insider threat is very real and very likely. The employees must be able to recognize it and perhaps more importantly, they need very clear procedures on how to report suspicious activities. (This is very important since I have assessed many information security programs and very few have well defined procedures to report suspicious activity).

Operationally the organization should be performing organization-wide risk assessments and security assessments. These will ensure that threats are recognized and many times aid in the discovery of insider threats.

Both operationally and technically, the organization needs to enforce two crucial concepts. The first concept is the separation of duties. This means that the person who approves an action, the person who carries out an action, and the person who monitors that action must be separate. This system makes malicious actions very difficult and is not only procedurally effective but hugely cost-effective. The second crucial concept is that of least privilege. Least privilege is providing an individual only enough access and tools to complete their duties. All persons with system access should have the least amount of privilege required to perform their business processes. Additionally data should be classified and the most sensitive data restricted with the concept of least privilege or "need to know". Password and account management practices must be in place. Accountability is the key. The organization must be able to trace any action back to a human being. Shared passwords or shared accounts undermine accountability and should never be used.

Revoking physical and logical access should happen prior to or during termination. It should not happen after, especially hours, days or weeks after. The organization should employ automated tools to ensure access is revoked as well as clearly defined procedures. Many cases of data theft happen after termination because the bad actor was able to retain access. Additionally, as part of least privilege and separation of duties the organization must make remote access account generation impossible without approvals and knowledge by others. Many times a person will know they are about to be terminated and will establish a separate log-on account to retain access; they must be prevented for doing so.

Retention of logs and investigative data is essential. Storage has become inexpensive enough that this should be organizationally required. Many times an organization does not discover it has been breached or a theft of data has occurred for months (unfortunately sometimes years) and without adequate retention of essential investigative data the organization may have little or no recourse. Investigation is nearly impossible without retention of logs and other relevant data.

Retaining data for investigation is one thing and retaining backups is another. The organization must have a fully functioning backup and recovery process. Theft of sensitive data can be damaging, however modification of data can be even worse. Imagine a major hospital which patient data is stolen. This would create a problem for the business of the hospital. If the patient data is altered it could result in death if a patient receives the incorrect treatment or medication. It is important to note that hospitals do employ several levels of control (check s and balances) to protect lives, but the point is that malicious insiders may have a motivation to hurt the company or people rather than steal the information. Having backups which retain integrity and the process to restore the data may play part in not only helping the business but may actually save lives.

And finally the organization must have clear and enforceable policies on what is and what is not acceptable when it comes to the confidentiality, integrity and availability of the organization's data. The policies and procedures of an organization put the organization at a legal advantage when pursuing action against the bad actor. Without them it is difficult to prove wrong doing or intent. This is a simple and inexpensive step which is extremely effective and important in the deterrence and prosecution of malicious activity.

Author bio

Damon Petraglia is the director of a demanding forensic practice and core to the leadership of a highly visible security program. He performs forensic examination and investigation, vulnerability analysis and risk / threat assessment, social engineering testing, security architecture review, incident response, and policy and procedure review and development.

EVIDENCE HANDLING FOR MOBILE DEVICES

Tips to consider when handling Mobile Devices

by Elias Psyllos, Senior Computer Forensic Analyst

Mobile devices are becoming more prevalent as evidence, in cases and investigations, whether it is for corporate or law enforcement. Mobile devices play a huge role in our everyday lives, so, the amount of data that passes through them can be extremely important for a case. No matter the reason or the matter, mobile devices should be handled with care. Improper seizure or handling of mobile devices can result in the destruction of evidence. There are some important tips to keep in mind about mobile devices that differ a little from the basic type of computer, laptop, and server evidence to which you may be accustomed.

Mobile devices can receive and transfer data from by different means; e.g. Cell Towers, Wi-Fi, and Bluetooth. You may be asking yourself, "Why is this important in handling Mobile devices as evidence?" The biggest mistake individuals make when they have mobile evidence is that they neglect to disable all the "Connections" on the mobile device.

We are at a point in time where mobile devices can be tracked, locked, and wiped remotely via our personal computers or applications that have been installed on the device. This causes huge concern for handling Mobile devices that have the wireless service enabled. Let's put a scenario together: You are on-site and have seized five mobile devices from two individuals, who you suspect are involved in the matter at hand. You place the mobile devices in evidence bags, put them in your briefcase, and take them back to the office. The two suspects are questioned and released, pending further investigation of their mobile devices. You log the mobile devices into an evidence lockup and go home for the night. In the morning you arrive back at your office, check the mobile devices out of evidence lockup, and realize that the devices have been wiped. You say to yourself, "That can't be. They were locked in evidence lockup all night in a secure area." The data that may have been vital to your case has just vanished. What happened?

This is a simple answer: You left the mobile devices connected to their networks and after questioning the two suspects, you released them, pending further investigation. In the meantime, the suspects went back to their homes, logged into their "trace and wipe" application and remotely wiped their phones, erasing all data.

This happens more than you may think, and in most cases, the data is lost for good. As an example, let's run through disabling the "wireless connections" on an iPhone.

1. Here is the screen of an iPhone you have just received as evidence in a matter.

2. You notice that the connections are still enabled by looking in the top, left-hand corner and seeing the phone is receiving service from AT&T. You then swipe the screen to unlock the phone (there is no pass code, you are lucky this time).

3. Select the "Settings" button, by gently taping the icon on the screen with your finger. You should then see the following menu appear.

4. The easiest way to disable all the connections is to switch "Airplane Mode" to "ON". Note: This does not disable WI -FI, so you will want to switch WI-FI to "OFF" as well. Once "AIRPLANE MODE" is activated, you will see in the top left corner, where AT&T used to be, a picture of a plane (as seen below).

5. The phone is no longer receiving any type of service connection, there is no way for it to receive a remote wipe command or lock the phone out.

By placing the phone into "AIRPLANE MODE," we can now securely create a forensic image of the mobile device for further analysis, ensuring the safety of the data residing on the mobile device.

The important thing to keep in mind is that the iPhone is not the only mobile device that has these features. As mentioned previously, there are different programs and applications for mobile devices that allow users to do the same. At the same time, older mobile devices may not have a WI-FI feature or an Airplane Feature. In such case, pull the battery out of the phone; before doing this, ensure there is no pass code enabled.

Always ask the suspect if there is a pass code and if they will provide it to you. Test the pass code while onsite to ensure it is correct. Once the pass code has been verified, remove the battery—this will ensure no signals reach the phone. Another option to pulling the battery is to place the phone in a Faraday bag or box. A Faraday bag or box is a special bag or box that keeps any signals from entering or leaving the mobile device. (The image, below, is of a Faraday box. Notice the round holes, those are actual gloves so you can still work on the mobile device without risking any signals reaching the device. There is also a power cord inside to keep the device powered and USB jacks on the outside of the box to connect the device to the Mobile Forensics tool of your choice.)

This means you can keep the device on and not have to worry about signals reaching the phone to wipe it.

This is a forensically sound option, especially if you are unsure about pulling the battery, or are unable to determine if the device has a pass code, or cannot retrieve the pass code

Now that we have cut off all signals and service to our mobile device to protect the data, we next want to focus on correctly documenting the mobile device's information.

It is important to document the following items on your Chain of Custody document (a Chain of Custody document tracks the whereabouts of the evidence and who has handled the evidence throughout its life cycle, beginning from when it was seized or received):

1. Make and model of the Mobile device. (This information can be found under the battery on the phone. Simply remove the battery cover and battery; you will see a label displaying this information.)

2. Is there a SIM card present and, if so, how many (note: not all mobile devices have SIM cards)?

3. Is there a Secure Digital (SD) or memory card present?

4. Document the IMEI or ESN number (Note: IMEI stands for International Mobile Equipment Identity and ESN stands for Electronic Serial Number. This information can be found under the battery on the phone. Simply remove the battery cover and battery; you will see a label displaying this information.)

5. Is there a pass code and, if so, what is it?

6. Have you disabled all connections possible that would allow the mobile device to send or receive signals?

7. Are there any chargers or data cables associated with the mobile device?

(Note: It is very important to also seize the power cables and data cables associated with the mobile device, since you might need these later for imaging purposes.)

The items listed may not be everything you want to document but can be used as a guideline for the type of items you want to document about your mobile device.

Once this is all complete, ensure that you place all mobile devices and associated items in a bag and seal the bag. Whether you are with corporate or law enforcement, the "bag and tag" method is a great way to ensure that no one has physically tampered with the evidence and, also, shows the Chain of Custody of the evidence.

Make sure any access to the evidence or assignment to a new person is documented in the Chain of Custody document. If the matter ends up going to court, the Chain of Custody document will be requested. This will allow the court and the individuals involved in the court proceedings to understand the life cycle of the evidence. If anyone questions the handling or responsibility of the evidence, the Chain of Custody will be able to answer these types of questions.

Mobile devices are ever-evolving media. Taking special care in handling them is important in safeguarding and ensuring the validity of the data contained within the mobile device. Each device is different, whether it is a different operating system or different software version. These are all factors that contribute to the successful, forensic imaging of these devices. While each device might differ from the next, effecting standard operating procedures for handling the devices can be tremendously beneficial.

This article is the first of a series of articles to be written that focus on forensically handling and acquiring Mobile Devices.

Electronic Evidence
Computer Forensics
Legal Technology

November 12th, 2012
Clarion Congress Hotel, Prague
Czech Republic

EVIDENCE HANDLING FOR DIGITAL MEDIA

Tips to consider with DM like computers, thumbs drives and servers

by Elias Psyllos, Senior Computer Forensic Analyst

Evidence handling is considered one of the most important aspects in the entire forensic investigation process; it is the first interaction between the Forensic Analyst and the evidence. The first steps in handling evidence ensure the integrity of the digital media throughout its evidentiary lifecycle. Evidence handling is also one of the first topics discussed, if the evidence ends up in court proceedings. If the evidence is not handled properly, it can be dismissed from being used in a court.

When entering a situation that will involve handling of digital media, the first step should be to photograph the location in which the potential evidence is located. Photographs show a 360-degree view of the location, prior to taking any action. This allows the analyst to depict the location as found upon arrival. The second step involved with evidence handling would be to photograph the digital media in question.

The following photographs should be taken of the digital media:

- 360-degree pictures of the Digital Media. (Note: Place a non-sticky tag on the digital media, showing the evidence name and number that should be depicted in each photograph taken.)
- Digital Media's make, model, and serial number tag(s).
- If the digital media is powered on, take photographs of the digital media's monitor.

- Photographs of all the cables plugged into the digital media (if applicable).

- Depending on the scenario, if on-site imaging will take place, then 360-degree photographs of the location, digital media, and cables should be taken upon completion of imaging. The photographs should be compared to the original photographs, to ensure the location and digital media is exactly as it was upon arrival.

Photographs also assist the Forensic Analyst in depicting the scenario at that time. For example, if the analyst is being questioned two months after handling the evidence, he or she can refer to the photographs as needed to retrieve details.

A vital next step in the handling of digital media involves the Chain of Custody document(s). It is the documentation associated with tracking all aspects and details of the digital evidence. This document should cover the following items, plus any additional information you find necessary:

1. Details of Investigation:
   - Location of Investigation
   - Case Number/Name
   - Evidence Number
   - Name of Forensic Analyst
2. Details of the Digital Media:
   - Make & Model
   - Serial Number
   - Was the device powered on or off?
   - Is it encrypted?
   - Size of hard drive or memory
   - Location of digital media
   - Local Time & Date
   - BIOS time and date (if applicable)
   - Operating System
   - Owner/User of digital media
3. Details of Imaging
   - Tool(s) used for Imaging
   - Type of write-blocking device used (if applicable)
   - Physical or Logical Image
   - Start Time and Date of Image
   - End Time and Date of Image
   - Evidence Name and Number
   - Digital media's hard drives make, model, and serial number that will be imaged (if applicable).
4. Details of Verification
   - Did the image verify? (Note: If the image does not verify, make sure to note the reason.)
   - What is the MD5 hash value?
   - Start Time and Date of Verification
   - End Time and Date of Verification
   - Tool Used to Verify
5. Details of Chain of Custody: This part of the form will track the physical access to the evidence throughout the lifecycle. It should include items such as:
   - Name
   - Professional Title
   - Date and Time
   - Company/Organization name
   - Location
   - Evidence Ownership Date
   - Signature

The Chain of Custody document should be completed up to the "Details of Imaging" section, prior to physically beginning the evidence-handling process.

Essentially, two possible scenarios exist, when dealing with handling digital media evidence. The digital media are either powered on or off at the time the Forensic Analyst gains possession of the media. This will determine how the analyst proceeds in his investigation. If the digital media is powered off, the following steps should occur:

- Pull the power cord from the outlet to prevent any power from reaching the digital media. If the digital media has a battery, such as a laptop, remove the battery as well.
- Physically access the hard drive (if applicable) and place an evidence label on the hard drive.
- Take photographs of the hard drive with the evidence label; documenting the make, model, serial number, and data size of drive.
- No matter what software is being used to image the drive, first, connect the drive to a write-blocker. A write-blocker allows the Forensic Analyst to read the hard drive (or digital media: thumb drive, external hard drive, etc.) with their software, but not write any information to it, preventing the evidence from possibly being altered or corrupted. The picture below depicts a set of Tableau write-blockers, each of which has different connections for digital media (Note: The yellow write blocker is actually a read/write-blocker).

If forensic hardware is being used, such as a Tableau TD1, the forensic hardware should have a write protection feature. Below is picture of a Tableau TD1. (Note: The Tableau TD1 is write-protected hardware and allows the Forensic Analyst to create a forensically sound image of the hard drive.)

- Ensure that the destination media, used to store the forensic image, has been forensically wiped, to ensure no previous data resides on the drive.
- Once the hard drive (or digital media) imaging has finished, the forensic image must be verified to ensure an exact duplicate was created. (Note: Software like FTK Imager, allows the Forensic Analyst to select imaging and verification at the start of the process so that once the image has been created, the verification automatically starts. The verification will compare the MD5 hash value of the hard drive (or digital media) and the forensic image to ensure they are an exact match.)
- Once the verification has completed successfully, the hard drive can be place back into the original computer.
- The rest of the Chain of Custody form, starting from "Details of Imaging," can be completed.
- Follow the steps described in the Photography section above, again, and compare the originals pictures to the com-

plete pictures to ensure all items are as they were upon arrival.

If the digital media is powered on, the following steps should occur:

- Before pulling the power cord out of the outlet and removing all power to the computer, it is vital to review the computer for encryption.
- If no encryption is present, the Forensic Analyst can follow the steps listed above for a Powered Off mobile device. However, if encryption is found to be present, the Forensic Analyst, should consider performing a Live Image of the digital media.
- If the Digital Media is unlocked (the user has signed into their account), then, performing a Live Image will allow the Forensic Analyst to bypass the encryption and create an unencrypted forensic image of the digital media.
- In this scenario, bootable software would be required. Installing software on the digital media is considered altering the evidence and is not considered best practice for forensic imaging purposes. FTK Imager Lite is a type of forensic imaging software that can be booted from a thumb drive or CD/DVD disc. It will allow the analyst to create a physical or logical image of the hard drive while the computer is running by simply attaching the destination drive to the computer and pointing FTK Imager Lite to the destination drive.
- FTK Imager Lite will also verify the forensic image and produce a report (which is automatically saved to the destination drive) showing the verification of the MD5 hash values.
- Once verification has completed, the Forensic Analyst can continue to follow the steps mentioned above (for powered off devices), starting at Step 8.

There are many types of digital media and each scenario will differ from the next, but having a strong understanding of evidence handling is a important for successful forensic acquisition. Remember, this first, crucial step in the entire life cycle in an investigation determines the validity and proof of the image being an exact copy of the original evidence.
This article is the first of a series of articles that focus on forensically handling and acquiring Digital Media.

Author bio

Before entering the Computer Forensics arena, Elias was in the financial sector as a Financial Analyst. He has five years Computer Forensics experience and has served as a Sr. Forensic Examiner and Team Lead. Elias has vast experience with conducting forensic acquisitions on digital media and mobile devices. He, also, has experience conducting targeted, multi-user, and small- to large-scale collections and analysis. Elias has worked in both the Corporate and Federal Law Enforcement Agency side of Computer Forensics. Elias has conducted digital forensic investigations for Fortune 500 corporations, Amlaw 100 law firms, large and medium financial institutions and corporations, non-profits, and law enforcement agencies. Elias is a seasoned Sr. Forensic Examiner with extraordinary project management and client-interfacing skills that are utilized for any size matter.

ISSE

INTEGRATED SAFETY & SECURITY EXHIBITION

LEADING NATIONAL SAFETY & SECURITY EXHIBITION IN RUSSIA

INTEGRATED SAFETY AND SECURITY EXHIBITION

2013

May 21-24

Moscow,
All-Russia Exhibition Center, Hall 75

- Protection & Defence
- Technical Facilities for Border and Customs Control
- Security Technical Systems and Equipment
- Fire Protection
- Rescue Equipment
- Disaster Medicine
- Environmental Safety
- Industrial Safety
- Equipment for Nuclear, Chemical and Biological Safety
- Information and Communication Security
- Transport Safety

www.isse-russia.ru

Organizers:

Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequencies of Natural Disasters (Emercom of Russia)

Ministry of the Interior of Russia

Federal Service of Military-Technical Cooperation

A SHORT INTRODUCTION TO STATIC MALWARE ANALYSIS

by Jan Goebel

In this article, we present a short guide on how to get an overview of a malware's functionality through static analysis. We also briefly show how the usage of IDA scripts can facilitate the analysis process by presenting a deobfuscation routine to reveal obfuscated strings of an example binary.

WHAT YOU SHOULD KNOW

- The reader should have a basic understanding of the Windows API and what it is used for, as well as, basic knowledge of PE header information. The reader should also be familiar with IDA disassembler and some basics on assembly language.

WHAT YOU SHOULD LEARN

- The reader should learn basic steps on how to briefly analyze a malicious binary in order to get an overview of its main functionality as well as network indicators to be able to detect other infected systems on the network.

Malware has become an almost tolerated threat of the Internet. Private hosts and enterprise clients get compromised every day and the number of files to analyse is growing constantly. Automated sandbox systems have evolved to counter this threat, but they are not always the solution of all problems. Thus, knowing how to manually investigate a malicious binary and obtain the most important information must not be forgotten.

INTRODUCTION

Malware Forensic, or Malware Analysis as it is often called, is the process of dissecting and understanding the functionality of malicious software (short: malware). As in most cases the actual source code of such a malicious program that needs to be analysed is not available, investigators need to apply different techniques in order to get an understanding of a particular piece of malware. These techniques can be roughly divided into static and dynamic analysis techniques. However, there is no single tool or technique that can be used at all times to analyse malware, it is always a combination of different tools and techniques.

In this article, we provide a short introduction to static malware analysis techniques, that help to get a quick overview of the basic functionality of a malicious program. That means, we do not run it in a debugger or execute it in a monitored environment, but only investigate the binary file itself. For this purpose, we took a real malware binary found in the Internet and present a step by step investigation on how to find out most of its functionality and main forensic indicators in order to detect other infected systems on the network.

MALWARE ANALYSIS

In our day to day business as security researchers, malware analysts, or incident handlers, we are almost always confronted with malicious executable files that need to be analysed. But what is the purpose of analysing such software?

The reason to analyse such files, for example, from an incident handlers point of view, is to discover as much infection indicators as possible to detect other compromised machines on the network. In this context it is important to find network indicators, such as command and control servers or custom network protocols to search the network for further infected clients and also to get an overview of the extent of the infection. For this reason, we need to know what a piece of malicious software does on a system and how it interacts with its environment.

In this article we take a closer look at a malicious file with the MD5 fingerprint d5f6623e2a6240bcca7b3f4086e8c539, which we discovered on a computer in April 2012 (first public information in the Internet appear in August 2012), and describe the tools we used to get a quick overview of what traces it leaves on the filesystem and on the network.

FIRST ANALYSIS STEPS

One of the first steps before digging deeper into a piece of malware binary is to create an MD5 fingerprint, e.g. using *md-5deep*[1] on Unix-based operating systems. These fingerprints are commonly used to uniquely identify the file and search for information about it on the Internet. Websites like *VirusTotal*[2], allow for example to search their database of collected malware by MD5 fingerprints. As a result, one can determine if a discovered malware is already widely known to the anti-virus vendors or not. Especially in the context of advanced persistent threats (APTs), the malware used by the attackers will be only limited to a small set of victims and therefore the number of information on those files in the Internet will be likely zero. In this case, the malware seems to be rather mass-malware, since it is well known and widely detected by anti-virus products (see results at VirusTotal) as some kind of generic backdoor or proxy trojan.

As a next step, we can use the tool *PEiD*[3] to find out if the file is packed in some way. Packers are used by malware authors to make static binary analysis more difficult. PEiD is a small Windows tool, that provides signatures for several different packers commonly used by malware. Figure 1 shows an example output of PEiD for the file we want to analyse. Besides the packer detection, PEiD also provides some hints on which programming language was probably used. This is especially helpful when analysing binaries in the disassembler *IDA*[4] and want to apply code signatures to distinguish custom code from well-known library functions.

Another tool that also provides useful information to the analyst is called *exiftool*[5]. It is a Unix tool that provides meta information on files of different types. In case of executables, we are for example able to retrieve the date the file was compiled (Time Stamp), its last modification time (File Modification Date/Time), and the code entry point (Entry Point). The full output of exiftool for our malware binary is shown in Listing 1.

```
00403151 var_60          = byte ptr -60h
00403151 StartupInfo     = _STARTUPINFOA ptr -5Ch
00403151 var_18          = dword ptr -18h
00403151 var_4           = dword ptr -4
00403151
00403151                 push    ebp
00403152                 mov     ebp, esp
00403154                 push    0FFFFFFFFh
00403156                 push    offset unk_4040F0
0040315B                 push    offset loc_4032E0
00403160                 mov     eax, large fs:0
```

Figure 1: PEiD output on malicious binary

```
> exiftool d5f6623e2a6240bcca7b3f4086e8c539
ExifTool Version Number         : 8.80
File Name                       : d5f6623e2a6240bc-
ca7b3f4086e8c539
Directory                       : .
File Size                       : 14 kB
File Modification Date/Time     : 2012:05:29
16:23:45+02:00
File Permissions                : rw-r--r--
File Type                       : Win32 EXE
MIME Type                       : application/oc-
tet-stream
Machine Type                    : Intel 386 or la-
ter, and compatibles
Time Stamp                      : 2012:04:13
08:27:59+02:00
PE Type                         : PE32
Linker Version                  : 10.0
Code Size                       : 9216
Initialized Data Size           : 4096
Uninitialized Data Size         : 0
Entry Point                     : 0x3151
OS Version                      : 5.1
Image Version                   : 0.0
Subsystem Version               : 5.1
Subsystem                       : Windows GUI
```

Listing 1 *Output of exiftool of an executable file*

We can also gather additional information when analysing the PE header of an executable. For this purpose there exist several different tools, such as PE *Explorer*[6] for Microsoft Windows or *pefile*[7] for Unix. There are two very interesting parts when analysing the PE header: the import section and, especially in case of dynamic link libraries (DLLs) the export section. The import section contains information about what system libraries and functions are imported and allow us to get an overview of the capa- bilities of a malware. For example, if the library WS2_32.dll is imported, we know that the malware is very likely communicating over the network. The export section contains functions that are exported by an executable, thus it might give us a hint about different entry points. Listing 2 shows a shortened list of libraries and functions that are imported by the malware file we are analysing.
From this rather short list, we can get a first impression of the malware functionality. We know it uses threads (CreateThread), it can write files (fopen, fwrite), probably to a temporary directory (GetTempPathA), it has network functionality (WS2_32.dll), and it can mess around with Windows services (RegisterServiceCtrlHandlerW). Note that for the network library WS2_32.dll no functions are listed, because in this case they are imported by ordinal and the tool we used to list the entries is not able to resolve those to the real functions. We will later see that for example IDA can resolve the correct function names.

1. *http://md5deep.sourceforge.net/*
2. *http://www.virustotal.com*
3. *http://peid.has.it/*
4. *http://hex-rays.com*
5. *http://owl.phy.queensu.ca/ phil/exiftool/*
6. *http://www.heaventools.com/*
7. *http://code.google.com/p/pefile/*

```
KERNEL32.dll
        Function: GetTempPathA
        Function: CreateThread
MSVCRT.dll
        Function: fopen
        Function: fwrite
        Function: memcpy
        Function: malloc
WS2_32.dll
ADVAPI32.dll
        Function: RegisterServiceCtrlHandlerW
       Function: StartServiceCtrlDispatcherW
```

Listing 2 *Shortened list of libraries and functions imported by the malware*

To enrich the gathered information with further data we use the Unix tool *strings*[8] to extract all printable characters from the binary. This also reveals a lot of the information we already know, such as imported functions, but it sometimes also provides additional information, such as file names or URLs. In this case, we can obtain some very interesting character strings from the binary, which are shown in Listing 3.

```
ProxyBot.exe
CONNECT
Host:
ftp://
```

Listing 3 *List of most notable character strings found in the malicious binary*

These character strings give use more information about the network functionality of the malware. The word CONNECT, for example, is a command from the hypertext transfer protocol (HTTP) and tells us that the malware is HTTP proxy-aware, i.e. it can use a HTTP proxy to connect to the Internet or might as well itself provide HTTP proxy capabilities. This assumption is reinforced by the file name ProxyBot.exe, which suggests that this piece of malware itself might function as a proxy or that it is capable of using a proxy. Finally, the word ftp:// gives us the hint, that this malware might also use the file transfer protocol (FTP) to transfer data. However, we do not yet know the command and control domains of this malware, i.e. to what network location is the malware connecting, which is important to detect other compromised machines.

From the output of PEiD we know that the malware is not packed or crypted, thus it might be that network related information is obfuscated in some way. To find out whether an obfuscation technique is used to hide valuable information we need to open the malware binary in a disassembler, such as IDA.

IDA DISASSEMBLY

If we open the malware in IDA, we will end up with some disassembled code as shown in Figure 2, which shows the entry point of the executable file.

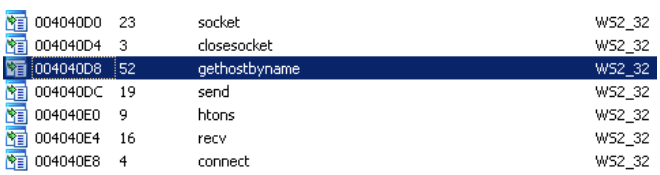


Figure 2: Entry point of malicious binary disassembled with IDA

8. *http://unixhelp.ed.ac.uk/CGI/man-cgi?strings*

Since we already know that the software has network functionality and want to find out where it is connecting to, one of the first steps is to check where in the code the appropriate application programming interface (API) calls are executed. For this purpose, IDA provides a subview called Imports, which lists the imported functions and libraries, most of which we have already seen during our first analysis in the previous section. Additionally, IDA can resolve the names of functions which are imported by their ordinal number instead of their name, thus we can see what network functions are used. Figure 3 shows the import subview of IDA and the network functions used by the malware. We already highlighted an interesting function named gethostbyname, which is used to resolve hostnames to their corresponding internet protocol (IP) address, thus it should receive a command and control domain as input. We can directly jump to the location where this function is imported and from their to the code locations which make use of it, by using so-called xrefs (cross-references of IDA).

Figure 3: IDA view of imported libraries and function

Following those cross-references and moving along the disassembled code, we will sooner or later stumble across an interesting looking function, which receives different offsets into the data section as input. Figure 4 shows the main loop of this function. This loop iterates over a character set (beginning with s5dk...) and modifies each byte at the provided offset by using the exclusive or (xor) operation. This seems to be the deobfuscation routine we have been looking for to reveal the network addresses of the command and control server.

```
00405414 unk_405414      db    0
00405415                 db    0
00405416                 db  10h
00405417                 db    0
00405418                 db  5Eh ; ^
00405419                 db  11h
0040541A                 db  1Bh
0040541B                 db  5Fh ; _
0040541C                 db  44h ; D
0040541D                 db  0Eh
0040541E                 db  56h ; V
0040541F                 db    4
00405420                 db  25h ; %
00405421                 db  20h
00405422                 db  65h ; e
00405423                 db  57h ; W
00405424                 db  59h ; Y
```

Figure 4: Deobfuscation loop

In order to deobfuscate the embedded character strings of the malicious binary without running it and grabbing them from memory, we need to write a small script for IDA. If the IDA Python plugin is installed, we can write such scripts in Python otherwise in C. Listing 4 shows an example Python IDA script that can be used to deobfuscate the character strings within the malware binary. Note that a closer look at the obfuscated character strings revealed, that the first byte always represents the length of the encoded character string. Thus, we

first retrieve the length and then iterate over each following character and xor it with the next character of the key. In case we reach the end of the key array we start at beginning again until the number of characters that have been deobfuscated reaches the length retrieved in the beginning.

```
# Imports
from idautils import *
from idc import *
import struct
# Get current EA
ea = ScreenEA()
# XOR Key Array
k = [,s',’5’,’d’,’k’,’6’,’7’,’f’,’7’,’j’,’L’,’K’,’K
’,’4’,’6’,’J’,’I’,’8’,’4’,’E’,’D’]
# Get String Length
codeLength = Byte(ea)
ea += 1
keyIndex = 0
counter = 0
# Loop over String
while True:
        currentKey = struct.unpack(,B’, k[keyIn-
dex])[0]
        currentByte = Byte(ea)
        newByte = currentByte^currentKey
        PatchByte(ea, newByte)
        keyIndex += 1
        keyIndex = keyIndex % len(k)
        ea += 1
        counter += 1
        if counter>=codeLength:
                break
```

Listing 4 *IDA Python script for character string deobfuscation*

Figure 5 shows one of the obfuscated character strings before applying the Python script from Listing 4 and Figure 6 shows the corresponding deobfuscated character string, which is one of the command and control domains (skupishanik.com). If we apply the IDA Python script on all obfuscated strings that we find in the data section, we discover a lot more useful information.

```
00405414 unk_405414       db    0
00405415                  db    0
00405416                  db  10h
00405417 aSkupishanik_co db 'skupishanik.com',0
00405427                  db    0
```

Figure 5: Obfuscated character string found in malicious binary

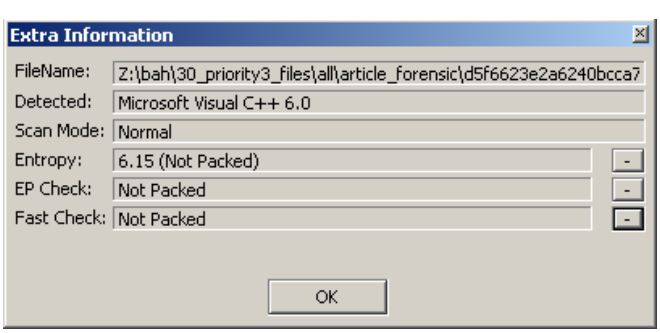


Figure 6: Deobfuscated character string showing one of the command and control domains

In total the malware contains four different command and control domains, namely: huvchik.com, nubasar.com, fhabefas.com, and skupishanik.com. From the other character strings, we can determine that the malware is capable of proxying HTTP connections (Proxy-Connection: Close and HTTP/1.0 200 Connection established), that it writes itself to a file named comsrvr.exe, creates a service with the name COMServer, and that it creates a registry entry at Software\Microsoft\Windows\CurrentVersion\Run to be started at automatically after reboot (persistence). Thus, we were able to verify most of the assumptions made in the beginning of this article, without ever running the malware binary. Of course, this was a rather simple example, but in most cases one can get a fairly good picture of the functionality of malicious software by looking at the embedded character strings, metainformation, and import and export sections.

CONCLUSION

In this article, we presented a common approach to manually analyse a malicious binary, without the need to execute it. We presented a few freely available tools, that greatly support this process and provide us with valuable information to get a quick overview of a malwares' functionality. With more complex examples this number of information will decrease, but it might still be enough to aid a forensic investigation or support the incident handler to find other compromised machines. Furthermore, it is still possible to extent the investigation, for example, with automated sandbox analysis or debugging. However, covering those topics is out of the scope of this short introduction.

Author bio

Jan Goebel graduated from RWTH Aachen University and received a Doctorate in Computer Science from Mannheim University. His research interests revolve around IT security, digital forensics, malware analysis (reverse engineering), and network attack detection using honeypots. Since 2011 he is working as a forensic expert and malware analyst for the Siemens CERT.

MASTER BOOT RECORD MALWARE ANALYSIS

by Patrick Olsen, BJ Gleason

Master Boot Record (MBR) malware is making a return. Once confined to floppy disks, the technique is now being used to install botnet-based rootkits. In this article, we will show you the basics of how MBR malware is deployed, how it installs itself, and how you can start to analyze what it is and what it is doing.

WHAT YOU SHOULD KNOW

• The reader should know how to use Virtual Machines and how to properly handle live machine.

WHAT YOU SHOULD LEARN

• From this article you will learn how to unpack malware, modify binary executables and analyze MBR malware.

The MBR is typically the first sector read by the ROM BIOS on a bootable device. The classic, original MBR is a 512 byte sector that contains the code to start loading the operating system into memory, and up to 4 primary partition tables. Over the years as the size of storage increased, the layout and utilization of the MBR has changed, see http://en.wikipedia.org/wiki/Master_boot_record for more details and additional examples.

While there have been changes, the basic functionality of the MBR remains the same - to load the operating system from the disk to the system RAM, and therein lies it's weakness. If we can change the MBR, we can introduce malware below the OS, modifying the OS as it is loaded, and change the way the system behaves. This process, known as rootkiting is often difficult to detect, as the system tools of the OS have been modified not to reveal any details about the rootkit.

How can the MBR on system be subverted? There are many classic ways - booting from an infected device (USB, CD, Floppy, etc.), downloading an infected executable, or visiting a infected website. In each case, once the system runs the payload, it modifies the MBR, and then starts executing the payload.

One of the first internationally-recognized boot record attacks was the Michelangelo computer virus (a variant of the Stoned virus). It was first discovered in 1991, and grew to stature in early 1992 when it was discovered that it had infected system and software being shipped from the factory. It infected MS -DOS systems, and if the system was active on March 6, the virus would overwrite the first 100 sectors of the hard disk with nulls, typically wiping out the file allocation table and part of the OS, rendering the system un-bootable (http://en.wikipedia.org/wiki/Michelangelo_(computer_virus)). The virus was actually easy to detect, as it didn't really install any measures to hide itself. A user could use the chkdsk command to detect

the virus, which would have reported 2048 bytes less than the actual installed memory. If you had 640k of RAM, chkdsk would return 655,360 on an uninfected system and 653,312 on an infected system [1]. Because of the widespread publicity several anti-virus companies released free or low-cost utilities to remove Michelangelo from infected systems.

There have been numerous attempts to protect the MBR, such as BIOS options to prevent changing it. The HP Workstation xw3100 [2] had an option to save the MBR to NVRAM, and on each system boot, it would check to see if the MBR had changed. If it had been changed, the MBR could be restored from the NVRAM. Some machines shipped with the Phoenix Award BIOS had Boot Sector Antivirus or MBR protection options as well [3]. These options typically prevented any changes to the current MBR. If you wanted to install a new OS, you would typically have to disable these options so that a new boot loader could be installed.

While MBR malware seems to be a very „old-school" approach to compromising systems from back in the days of exchanging floppy disk, there seems to be a bit of resurge going on now. According to Symantec, there has been a marked increase in MBR infections [4]. And not only are they back, they are doing so much more. Instead of just trashing your hard drive, they are being used for extortion (by encrypting the user's files and demanding payment for the decryption key), spam, insertions of back doors, and becoming part of a command-and-control botnet.

With this renewed interest in MBR malware, we decided to see how they actually attack and install themselves on your system by examining one in depth. What is the attack vector, how does it install a new MBR, and how does it hide itself from the system?

HANDS ON

As always, working with malware is dangerous as you could infect the system you are running the analysis on. It is highly recommended that you use isolated systems, not connected to any network, and run the analysis inside virtual machines. Before performing any forensic analysis of malware, I would recommend reading „5 Steps to Building a Malware Analysis Toolkit Using Free Tools" by Lenny Zelster [5]. His recommendation, in brief, is to use a virtual machine disconnceted from any production systems, and load it up with tools. Once the tools are loaded, take a snaphost of the virtual machine so it can be restored to a „pre-infected" state, wiping out any traces of the malware that was installed.

While there are many examples of MBR based malware out there, the one we will be looking at is this one:

http://contagiodump.blogspot.kr/2012/05/mbr-rootkit-xpaj-sample.html

The malware we are examining is supposed to be a crack for the „Stoked: Big Air" game, a snowboarding simulation game, available from http://www.bongfish.com/. The Big Air edition of the game added additional mountains, increased the frame rate, and added new racing events. The game garnered many favorable reviews, and earned a MetaCritic score of 81% [6].

According to Symantec, W32.Xpaj.B, is a new and improved version of W32.Xpaj and is considered a „file infector with a vengeance" [7]. Originally discovered in 2009, it has seen a resurgence starting in January 2012. It infects the MBR, attacks 32 and 64 bit versions Windows, and runs code in kernel mode. Bitdefender refers to this version of Xpaj as „the bootkit edition" [8].
You can download the sample malware, but the zip file is password protected, and you will need to contact the site operator for the password.

STARTING THE ANALYSIS

Since we are running inside a virtual machine, disconnected from any other systems, we could just execute the sample and see what happens. However, it is recommended we analyze the static binary and see what we can learn from it.

It is common for malware to be packed, the process of which makes static analysis harder. When examining malware it is typically a good idea to perform tests with different tools and compare the results to verify the information. In this first test we will use the manual approach using bintext [9] which extracts text from a binary file. This is similar to the strings command in Linux.

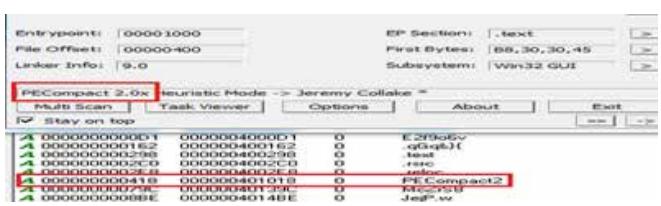


Figure 1 - Output of bintext

In the resulting output from Figure 1, we see the print „PECompact2". PECompact, is a commercial packer available from http://bitsum.com. Packers are not just used for malware, but can be used to shrink the size of an executable to make it fit on a smaller storage device, or to minimize download times. Once the packed file is executed, it is unpacked into RAM and then executed.

PEiD, from http://www.peid.info/, is a collection of automated tools that will detect a wide range of packers, but like anti-virus software, it's signature database needs to be updated on a regular basis. By design, PEiD will identify the packer but will not unpack the executable. However, there are several plug-ins available for PEiD that give it unpacking abilities.

When we examine the executable with PEid, what we see is shown in Figure 2.

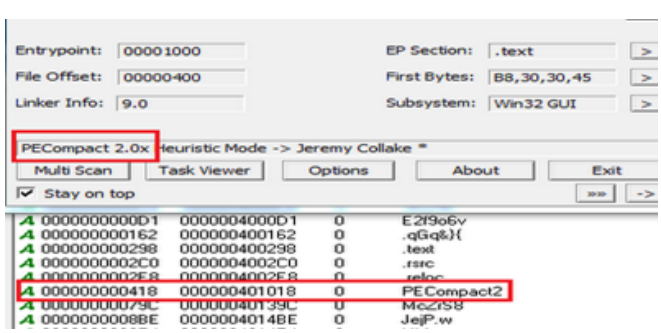


Figure 2 - Output of PEiD

The output from PEiD confirms that PXCompact 2.0x was used to compress this executable.

UNPACKING THE CODE

Knowing that the executable is packed, we need to be able to unpack the malware code so we can start to examine it and see what it does. While there are a number of ways this can be done, we will use Ollydbg to modify the executable to stop once it has unpacked the code, and before it has transferred control to the malware. The way most of these packers work is that once they are loaded into memory, they are pointed to the packed data and execute an unpacking routine. Once the data is completely unpacked, the unpacker jumps to the first instruction of the unpacked code.

Upon opening the program in Ollydbg we are dropped into the Original Entry Point (OEP) of PECompact, as in Figure 3. It's moving a value into EAX. One of the characteristics of PECompact is the JMP EAX, which is typically located close to the value being moved into EAX at the OEP. So what we will do here go to the expression, 00453030. You can do this by hitting the Ctrl+G key while inside OllyDbg. Then type 00453030 into the box.

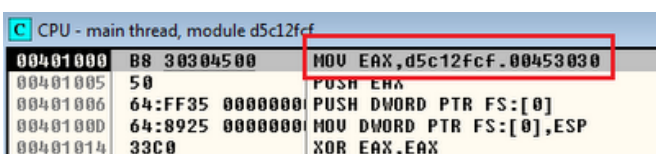


Figure 3- Starting Point in OllyDbg

After we go to expression 00453030 it will look like Figure 4: Note the address location in red.

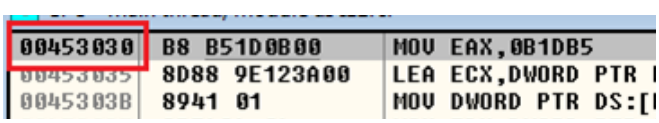


Figure 4- Starting Point

Now once you are here, scroll down and look for a bunch of POPs for EDX, ESI, etc. Right after all of those POPs you will have the JMP EAX that we talked about above. This JMP EAX in Figure 5 is where the unpacker will transfer control to the original, unpacked code. There are several things we can do at this point, such as setting a breakpoint, but instead, we will modify the JMP instruction, to create an infinite loop.

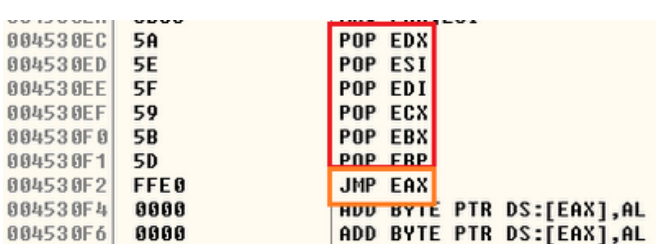


Figure 5- Transfer to unpacked code

The JMP EAX instruction takes up two bytes of memory, so any modifications we make can only use 2 bytes or less. It turns out that there is a JMP short relative instruction that can be used to jump –128 to +127 bytes from the current EIP value. Since the JMP EAX and JMP short are both two bytes long, we can replace one with the other. Now we just need to calculate where we want to jump to. When the JMP EAX instruction, located at 004530F2, is executed, the instruction pointer is incremented to 004530F4, however, the contents of the EAX registered will then be loaded into the instruction pointer, and the code at that address will be executed. We need to create an instruction that will basically, jump back two bytes, from 004530F4 back to 004530F2 so that we can create an infinite loop.

Since the operand for the JMP short relative uses a signed 8 bit notation, a '0' would be '00', a '-1' would be 'FF', and a '-2' would be 'FE' in hexadecimal. The opcode for the JMP short relative instruction is EB, so combining it, a JMP -2 would be EB FE. So if we replace the FFEO of the JMP EAX instruction with the EBFE of the JMP -2 instruction, we can execute the unpacking code, and once it has finished, it will sit in an infinite loop.

In Ollydbg, left click JMP EAX, and hit Ctrl+E, which will bring up a edit window as shown in Figure 6. You will want to change FE EO to EB FE JMP EIP, creating our infinite loop instead of transferring control to the unpacked executable.

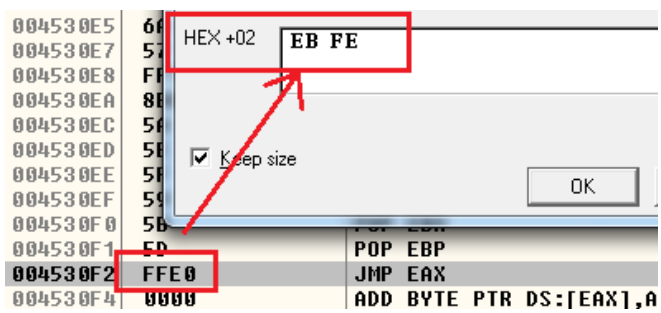


Figure 6- Inserting a JMP SHORT -2

After you make the modification, it should now look like Figure 7. The JMP SHORT instruction points back to itself, at address 004530F2.

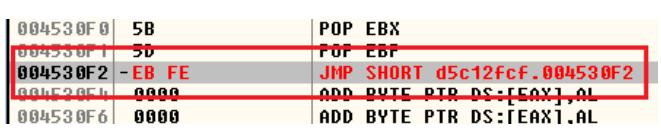


Figure 7- The infinite loop installed

You will want to right click the „red" code and select, „Copy to executable" and highlight „selection".

A window will pop-up that looks like Figure 8. Right click the window and select, „Save file".

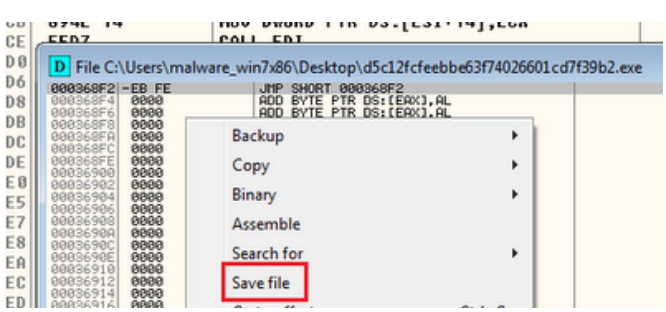


Figure 8- Saving the modified code

Save it as „loop.exe" or whatever you want, as shown in Figure 9.

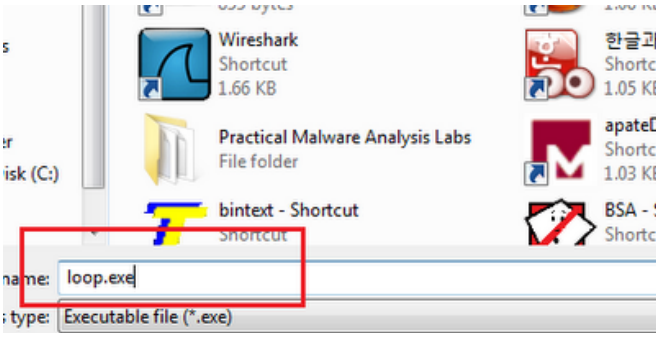


Figure 9 - Saving the code to disk

Now we have our edited exe file. Go ahead and close out of OllyDbg for now. Some malicious code can detect if it is being watched by debuggers.

Now we will execute the loop.exe. After it has executed, open up OllyDbg. Once OllyDbg is open, select File, highlight loop.exe and then select Attach, as shown in Figure 10. This will take you back into OllyDbg's „main screen".

Figure 10 - Attaching to a running executable

It will take you to a RETN, which is a return to 77C0F189, which is ntdll in Figure 11.

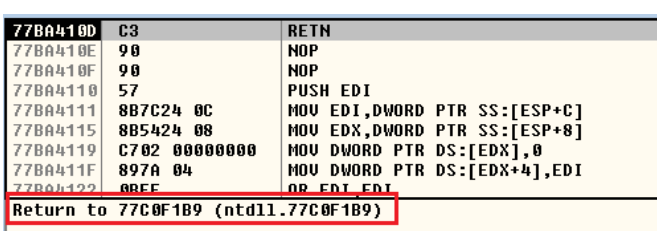


Figure 11 - ntdll

Hit F9, and then hit F12, which is a run and pause. It will drop you here shown in Figure 12. Look familiar? This is where we edited JMP EAX (FF E0) to JMP SHORT (EB FE). We will want to change this back to FF E0, so hit Ctrl+E and make the change.

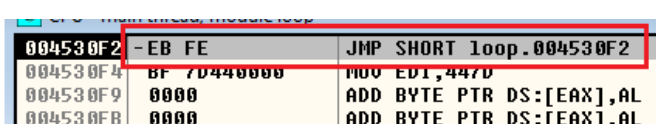


Figure 12 - Our infinite loop

Once this has been edited as shown in figure 13, you wil want to left click FF E0, and then hit F7 two times.

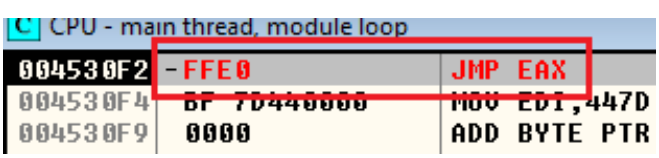


Figure 13 - Reverting to the JMP EAX

After you hit F7 twice you should be here in Figure 14: You can now dump the process using the Olly Dump Process plugin, or use LordPE.

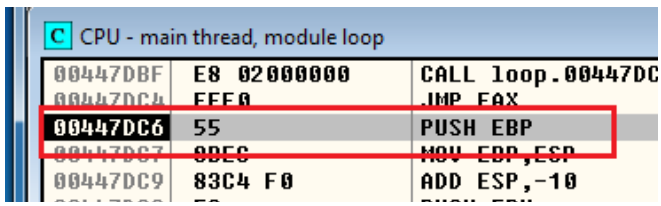


Figure 14 - Ready to dump the unpacked malware

EXAMINING THE MALWARE

Now that we have an unpacked version of the code, let's take a closer look at it. Let's see what it looks like compared to the previous packed version. Here is a quick view of the original.exe, and the dumped.exe that we dumped via OllyDbg. Hexacorn's hdive.exe [10] program really shows the differences as seen in Figure 15. We can also start to run the malware through other tools, such as a dissassembler, debuggers, and other tools to have it start revealing its secrets to us.

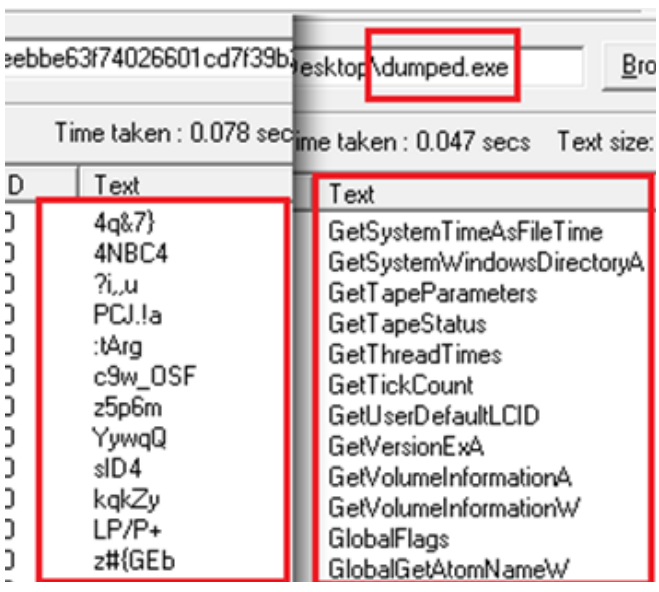


Figure 15 - Compressed vs. Uncompressed malware

CAPTURING THE MASTER BOOT RECORDS

As described before, the MBR is the first 512-byte sector. So that we can get a better idea what the malware will do it, let's get a copy of our current, un-infected MBR, which we can later compare with an infected MBR. We will use the dd command to save the MDR to disk. We will name it ombr.bin for Orginal MBR

dd.exe if=\\.\PhysicalDrive0 of=C:\Users\<username>\Desktop\ombr.bin bs=512 count=1 --localwrt

Once it is saved we can take a look at it, as shown in Figure 16.

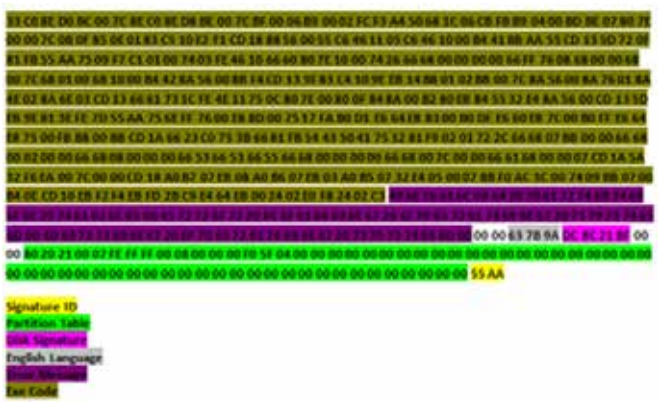


Figure 16 - Original MBR

There are some tools that you can use to take a closer look at what is going on in the MBR. There is MBRparser [11] by Gary Kessler Associates. This tools appears to use placement of partition tables to identify if malware might be hiding, but in this case it may get confused since the MBR was completely re-written. You can also try the MBR Parser [12] by Jamie Levy which seems to be designed to spot this kind of infection.

Figure 17 is the assembly code for the Original MBR we just extracted via dd and disassembled using MBR Parser.

```
000000 33C0                xor             eax, eax
000002 8ED0                mov             ss, ax
000004 BC007C8EC0          mov             esp, 0xC08E7C00
000009 8ED8                mov             ds, ax
00000B BE007CBF00          mov             esi, 0x00BF7C00
000010 06                  push            es
000011 B90002FCF3          mov             ecx, 0xF3FC0200
000016 A4                  movsb
000017 50                  push            eax
000018 681C06CBFB          push            0xFBCB061C
00001D B90400BDBE          mov             ecx, 0xBEBD0004
000022 07                  pop             es
000023 807E0000            cmp             [esi], 0x00000000
000027 7C0B                jl              +0x0000000B
000029 0F850E0183C5        jnz             -0x3A7CFEF2
00002F 10E2                adc             dl, ah
       ====================  ====================
       Error: unexpected byte at 000031
       The rest of the code contains 306 bytes
```

Figure 17 - Disassembly of the Original MBR

Now we will run dumped.exe and let it infect our system, after which we can grab another copy of the MBR.

dd.exe if=\\.\PhysicalDrive0 of=C:\Users\<username>\Desktop\imbr.bin bs=512 count=1 --localwrt

So we now have two copies of the MBR - the ombr.bin, Original MBR, and the imbr.bin, the Infected MBR.

If we compare the two files, we see a lot has changed. Figure 18 shows that we have similar patterns here, but it's nothing like the original one. The malware appears to replace the MBR with its own version.

Figure 18 - Infected MBR

Here is some of the assembly code of the infected MBR, in Figure 19. You will see that it's quite a bit more than the original MBR.

```
33C0            xor             eax, eax
90              nop
90              nop
EB10            jmp             +0x00000010
1000            adc             [eax], al
1200            adc             al, [eax]
0000            add             [eax], al
0020            add             [eax], ah
EC              in              al, dx
FF5F04          call            [edi+0x04]
0000            add             [eax], al
0000            add             [eax], al
31C0            xor             eax, 0x000000CC
8ED0            mov             ss, ax
BC007C8EC0      mov             esp, 0xC08E7C00
8ED8            mov             ds, ax
BE007CBF00      mov             esi, 0x00BF7C00
06              push            es
B90002FCF3      mov             ecx, 0xF3FC0200
A4              movsb
50              push            eax
683206CB88      push            0x88CB0632
16              push            ss
92              xchg            eax, edx
07              pop             es
FB              sti
6660            pushad
8B1E            mov             ebx, [esi]
4C              dec             esp
008E064E0026    add             [esi+0x26004E06]
66817F028801    cmp             [edi+0x02], 0x00000188
47              inc             edi
6D              insd            es:edi, edx
742E            jz              +0x0000002E
2E833E08        cmp             [esi], 0x00000008
06              push            es
0074260E        add             [esi+0x0E], dh
07              pop             es
A1130483E8      mov             eax, 0xE8830413
10C1            adc             cl, al
E006            loopnz          +0x00000006
A30C06E8A6      mov             0xA6E8060C, eax
007213          add             [edx+0x13], dh
31DB            xor             ebx, 0x000000CC
2666817F028801  cmp             [edi+0x02], 0x00000188
47              inc             edi
6D              insd            es:edi, edx
7506            jnz             +0x00000006
6661            popad
06              push            es
6A00            push            0x00000000
CB              retf
```

Figure 19 - Disassembly of the Infected MBR

If you open up the disk image in a hex editor you will see some interesting stuff. Take a look at the memory location offset and you will see that the MBR starts at 00000000. Note 7C00 in the assembly code, this is the memory address where it's loaded into memory; however, if you keep looking towards the end of the disk you will see some extra artifacts.

Starting at offset 8BFFF0400 you get the following:

It goes from 8BFFF0400 - 8BFFF059B.

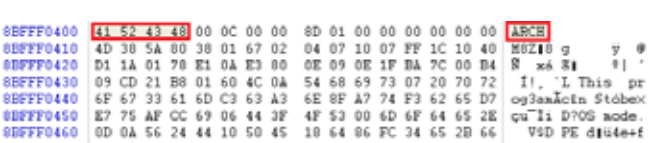


Figure 20 - Offset 8BFFF0400

Here you have it again from 8BFFF0800 - 8BFFF9BCB

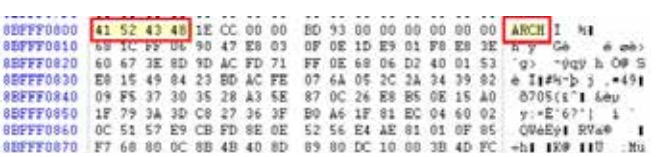


Figure 21 - Offset 8BFFF0800

There are also more hits at the following locations: 8BFFF9E00, 8BFFFB800, 8BFFFC929, 8BFFFE93A, 8BFFFF5F5. These various offset appear to be where various code segments are located.

They all appear to start with 41524348, which translates to ARCH, as seen in Figures 20 and 21, so this could possibly be an identity check. In either case, ensure you also check the end of your disk, and not just the beginning where you think the MBR should reside.

There also appears to be a clean (original) copy of the MBR located at 8BFFFFC00.

So it appears that the malware in this case makes a copy of the original MBR (just in case it needs any of the information inside it, and possibly if it receives a command to uninstall, it needed to replace the original MBR). It then starts rooting the host system and also attempts to contact a remote system.

For a more detailed description of the actual payload, please take a look at the excellent analysis at

- http://www.symantec.com/connect/blogs/w32xpajb-file-infector-vengeance
- http://www.virusbtn.com/pdf/conference_slides/2011/Lelli-VB2011.pdf
- http://labs.bitdefender.com/2012/04/xpaj-the-bootkit-edition/

PROTECTING THE NEXT GENERATION OF SYSTEMS

Preventing the installation of malware in the pre-boot phase has become a hot issue, and is being implemented in the next generation of PCs. Originally developed at Intel, the Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between the OS and the hardware, and is being developed to replace the current system BIOS. The many UEFIs being developed will allow for legacy BIOS support, and will allow for remote diagnoses and repair even without an operating system. The UEFI specification is managed by the Unified EFI Forum [13].

One of the key features of the UEFI is enhanced booting features that can be configured in the global NVRAM of the system. Instead of using a boot sector, the UEFI can retrieve the OS loader and drivers from standardized file systems and locations. For example, the OS loader would be loaded from \EFI\BOOT\BOOTx64.EFI off of a FAT based device.

In addition, the UEFI can have secure booting enabled, which would prevent access to the OS loaders or drivers that are not digitally signed, similar to digitally signed drivers in Window 7. This technique should prevent the injection of malware during the booting process. To help reduce the attacks on Windows, Microsoft is requiring systems certified for Windows 8 to have secure boot enabled by default, using the Microsoft private key. This raised some concerns that other non-Windows operating systems might be locked out of these machines, but Microsoft has indicated that they will allow the secure boot to be disabled or to enter the custom mode (except on systems based on the ARM processor).

CONCLUSIONS

MBR malware still exists and is still a danger. In this article we showed you some of the techniques you could use if you wanted to start analyzing how MBR malware works, how it installs, and what it could possibly do once it has taken control of your system. This is a serious enough issue that Intel and Microsoft are continuing to examine techniques that they can implement to eliminate this attack vector.

REFERENCES

[1] http://coast.cs.purdue.edu/pub/advisories/ciac/c-fy92/c-15.ciac-michelangelo-virus
[2] http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&taskId=130&prodSeriesId=346790&prodTypeId=12454&objectID=c00036617
[3] http://members.iinet.net.au/~herman546/p1.html
[4] http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion-infographic
[5] http://zeltser.com/malware-analysis-toolkit
[6] http://en.wikipedia.org/wiki/Stoked_(video_game)
[7] http://www.symantec.com/connect/blogs/w32xpajb-file-infector-vengeance
[8] http://labs.bitdefender.com/2012/04/xpaj-the-bootkit-edition/
[9] http://www.mcafee.com/us/downloads/free-tools/bintext.aspx
[10] http://www.hexacorn.com/blog/2012/06/07/hexdive-intelligent-string-extractor/
[11] http://www.garykessler.net/software/index.html
[12] http://gleeda.blogspot.kr/2012/04/mbr-parser.html
[13] http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

Authors bio

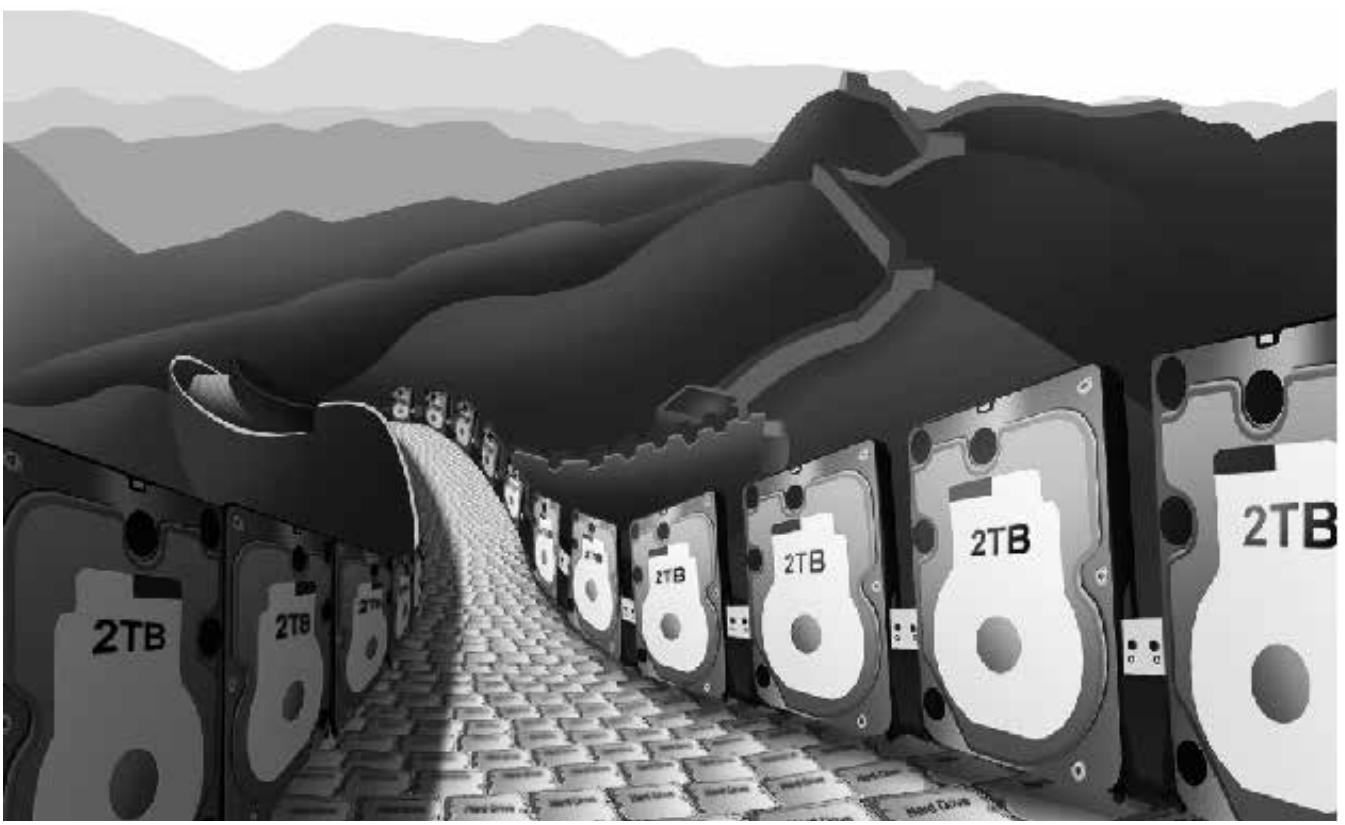
Patrick Olsen is currently supporting the Department of Defense (DoD) as a Computer Security Analyst. He has over 7 years of Information Security experience. He holds a BS degree from Bellevue University where he studied Security Management. He is the sole author of the blog; www.sysforensics.org. He also holds a CISSP, GREM, and CEH certification. He is also a member of the Consortium of Digital Forensic Specialists (CDFS) and High Technology Crime Investigation Association (HTCIA). He can be reached at patrickolsen@sysforensics.org

BJ Gleason has been teaching Information Technology and Computer Security classes for almost 30 years. He holds degrees in Computer Science, Criminal Justice, Asian Studies and Education. In addition, Mr. Gleason holds over 30 computer industry certifications from SANS, CISSP, and Microsoft and is a Certified Computer Examiner from the International Society of Forensic Computer Examiners. He came to Korea in 1995 for 2 months, met his wife and has never left. He is currently teaching for the University of Maryland University College in Seoul, Korea. He can be reached at bjgleas@gmail.com

COMPUTER FORENSIC CHALLENGES IN CHINA

By Erik Laykin Managing Director, Duff & Phelps LLC

Collecting Electronic Data in China is fraught with risks and challenges. In this article, computer forensics pioneer Erik Laykin shares some of his experiences and observations regarding the hurdles often faced when managing electronic data collections in this dynamic and emerging market.



The conviction and sentencing to 15 years in prison this month of Wang Lijun, the former chief of the 60,000-strong Chongqing (Chung King) Police force, on corruption and abuse of power charges in a Chengdu court marks a watershed event in modern Chinese politics. While Wang was a lightning rod in the city's anti-corruption crusade who directly and successfully took on the powerful Triads and deeply seated organized crime syndicates, what is generally not well known about him is that he was also one of China's major proponents of modern forensic science in criminal investigations and dedicated significant resources to developing capacity in this area.

As the co-chair of the 2nd Annual World Forensics Congress in Chongqing, China, last November, I worked with Wang who presided over our opening ceremonies and laid out his vision for a more thoroughly modern approach to managing and processing evidence. His emphasis was on establishing best practices throughout the region in the field of digital forensics and most specifically, electronic data harvested from the cloud.

To that end, according to Wang and his associates, they had engaged IBM, Dell, HP, Cisco and other major players in the traditional information technology space to help build out a sparkling new 100-million-dollar cloud computing, training, investigative research and analysis center on the grounds of the sprawling Chongqing Public Security Bureau campus.

The building was well under way last November when Wang arranged for me to have a VIP visit with him and his delegation. It was a significant project and was due to be completed in mid-2012. However, the Police Chief's February arrest followed the dramatic chase in which the now disgraced Chongqing Communist Party Boss and Politbureau member Bo Xilai sent 70 car loads of armed police after Wang, ending in a siege of the American Consulate in Chengdu where Wang had taking refuge. The future of his visionary effort to expand the field of forensics in China is currently in question.

None the less, policing agencies from Harbin to Ningbo have been very active in acquiring the necessary training and systems to provide rapid-response digital forensics to better address issues of both domestic state related security as well as criminal activity and economic disputes. Numerous American forensic firms such as Guidance Software and Logicube have focused on this market for years.

As a result, there has been a growing awareness throughout China that the proper preservation of digital data is a key component of any dispute or investigation.

This has not always been the case, and it is still the exception rather than the rule that electronic data will be entered as evidence in a Chinese court. This is in part due to the opaque nature of the Chinese legal system, wherein judgments and rulings are often predetermined long before arguments are made. Further, the notion that a defendant will mount an aggressive defense against the charges brought by the state are more fantasy than reality. By example, even Wang Lijun did not contest the charges against him and gave up his right to appeal despite the heavy potential penalty of death by execution which he was facing.

In practice, the usage of digital forensics in China by policing agencies is heavily weighted toward the surveillance, counter surveillance and investigative processes as opposed to the due process of law. By the time an investigation has been completed and referred to prosecutors, the outcome is likely well understood – at least by the state.

On the other hand, while digital data has been making its way into the filings in more commercial disputes, the vast majority of civil and commercial matters in China that rely on computer forensics are those that are subject to a foreign jurisdiction, notably the United States.

American commercial enterprises of every stripe operating in China - including FedEx, WalMart, KPMG, Mattel ,Home Depot and dozens of American law firms - have relied on the deployment of computer forensics for the purpose of managing a wide variety of risks and issues.

American firms have innumerable reasons to deploy computer forensic specialists in China. These range from the collection of electronic data in US-based litigation to managing internal investigations that may have been initiated by an inquiry from US regulators or even self-policing and auditing in accordance with efforts to prevent corruption or running afoul of the United States FCPA (Foreign Corrupt Practices Act).

In most cases, American firms are relying upon either dedicated in-house resources who have the requisite training and capabilities to manage data collections or on outside US or multi-national consultants whom are stationed in China.

These teams are required to operate within the framework of the Chinese legal system and must be aware of both local and national regulations guarding "state secrets" and other potential potholes that could in fact land a computer forensic practitioner in hot water.

Over the years, there have been numerous occasions where US-based computer forensic examiners were stopped at customs when entering China at the Beijing, Shanghai and Guangzhou airports only to learn that their equipment, hard drives and systems would be prevented from entering the country. In fact, in many cases, their systems were confiscated and not returned. Not a fun way to start a data collection project.

While these examples of customs officials taking a hard line on the importation of forensic equipment has waned as of recently, a forensic examiner always must be on the lookout for unknown and sudden risks.

In other cases, the export of collected data has proven problematic, especially if there is cause for local or national authorities to deem that data a "state secret." The interpretation of what constitutes a state secret has in some recent cases evolved to include what most American corporations would call "operating data and communications" such as E-Mail or management information regarding their own enterprise. This gray area causes concerns as interpretations of Chinese law are historically vague and at times conflicting, which introduces an element of unwanted risk. It is often hard to find definitive guidance on the propriety of any specific action that you may take with regards to the identification, collection, processing, hosting, import or export of electronic data. To that end, seeking guidance from local counsel or at the very least international counsel with familiarity of the issues is a prudent step and important component of any significant data collection effort in China.

By example, there is a school of thought in the world of Chinese forensics that emphasizes moving the collected data out of the country as quickly as possible to remove the risk of it being monitored, compromised or even claimed by authorities or even by the opposing parties in a legal action whom may have greater sway and influence with the local governing officials.

While these institutional risks and challenges exist and must be accounted for when developing an Electronic Data Collection Plan in China, there are other more immediate risks such as theft of equipment, physical accidents or the loss of team members. For example, I have had occasions where my forensic examiners have gone missing for days on end only to be found in Chinese police custody for questioning. In one such recent case, the examiner was picked up by Chinese customs officials on entering the country in what turned out to be a case of mistaken identity.

While my examiner was treated well while in Chinese custody, the fact that his whereabouts were unknown for five days was excruciatingly painful for his family. This also caused logistical challenges for our efforts on behalf of the client.

Other challenges in China range from the obvious language barriers to cultural nuances and challenges within information technology environments that are often less than ideal. All of these factors create a unique landscape which should be properly explained in advance to the party(s) requesting that the data be collected to properly manage their expectations.

The key to any successful data collection in China is preparation and maintaining a comprehensive understanding of the cultural and logistical limitations that must be managed at every step of the process.

You can not anticipate all of the possible twists and turns that a case may take, but you can take steps to remain nimble and aware of the environment that you are working within.

By example, on a China-based computer forensic collection our team was sent into the field to rapidly collect electronic data of the entire senior and mid-level management team of a major American company due to a US Federal Court order. However, after deploying, our efforts were quickly frozen due to the combination of two highly challenging events. First, we were impacted by the Chinese New Year, during which tens of millions of migrant workers flooded the nation's transportation system and infrastructure making their way home from every conceivable major city to every conceivable tiny rural village. This effectively shut our team out of the rail system in several locations and made air travel nearly impossible due to over -bookings. The second event was the untimely arrival of the worst snow storm seen in China in dozens of years.

While local and regional Governors and Ministers throughout China recognized that commerce and productivity would come to a standstill until these two colossal events passed, the Federal Judge sitting on the bench in the US would have none of it.

Our client questioned the delays to the process, our competence and even the availability of hard drives in places like Wuhan and Kaifeng China. Under pressure from all parties, our client simply did not want to accept the hard reality that a country of 1,300,000,000 people had basically come to a grinding halt.

Eventually, the snow cleared, the trains freed up and our work resumed its pace in cities far afield with names like Dalian, Chengdu, Tientsin, Yunnan and Xian - but the damage had been done. Despite all of the uncontrollable obstacles, I was still behind the 8 ball to please the court.

Sometimes the disruptions are comical such as when my team and I were left sitting in the taxi at the security gate of an electronics manufacturing plant in Shenzhen for 3 hours because nobody could make the decision whether to let us in the compound. The fact that we had arrived and were waiting entry on to the compound had to be escalated up to the Chairman, who was on holiday in America with his children who were visiting colleges for their dream of studying abroad. Considering our combined hourly rate, that was one expensive taxi ride.

Other challenges are just plain "old school," as you will have the occasional power outage midstream during an imaging job or employees will fail to provide you with their equipment, which has mysteriously disappeared just prior to our arrival on site.

But on the other hand, in countless cases over the years I have been fortunate to have the unequivocal support and assistance of the entire client team. Even in cases which are highly charged and involve theft of trade secrets, intellectual property disputes, internal fraud, corruption and other sundry acts.

What is interesting is that more often than not, the Chinese enterprise or foreign-owned-and-operated enterprise in China conducts affairs in a very Chinese manner, which is with a sense of mutual cooperation and an "everyone pitches in" attitude once the mandate has been set, argued, agreed upon and approved. The folks on the ground can actually move mountains despite the occasional stumbles, faux pas and quirks that seem to weave their way through any forensic collection exercise.

What I have learned from this is that detailed and active preparation for a computer forensic acquisition in China will ordinarily pay huge dividends. Taking the time to make sure that each of the stakeholders has signed on to and fully understands the mandate and the goal is critical. This often will entail detailed discussions and review of the approach, so as to bridge the many cultural, language and logistical disconnects that exist in even the best-laid plans and with the most eager and cooperative of clients.

It is important to understand that in China, it is not unusual for stakeholders or participants to hold back key information - not because of some fraudulent mal-intent, but because of deeply ingrained cultural proclivities that include the notion of "saving face." This could easily lead a mid-level manager to fail to disclose critical information for fear of impacting themselves or even their superiors.

As China's legal and regulatory landscape continues to evolve and mature, it will be incumbent on practitioners of computer forensics to stay well abreast of the most current interpretation of issues such as data privacy regulations, data export controls and any prohibitions on using specific tools or technologies within the country. It is not inconceivable that an uninformed forensic team could land themselves in regulatory hot water or even prison for failing to understand the limitations of what actions are deemed acceptable by local or national authorities. I would note that it is also not out of the realm of real possibility for a misunderstanding or misinterpretation of actions or intent to result in a local official taking a harsh line on the activity until it is later sorted out with other players in the state apparatus. This could result in your being the guest of the Chinese authorities for some undetermined amount of time. Thus, prudence and operating with caution is not only important but should be part of any team's standard operating procedure.

Author bio

Erik Laykin is a managing director at Duff & Phelps LLC, a NYSE listed international consulting firm founded in 1932. He is an electronic discovery/computer forensic authority and an internationally recognized testifying expert in the reactive investigation and analysis of cyber-crime, electronic fraud, data breaches, trade secret theft, trademark, patent and systems design infringement/failure, online piracy, corporate espionage and other complex information technology disputes.

About Duff & Phelps LLC

A leading global financial advisory and investment banking firm, Duff & Phelps (NYSE: DUF) balances analytical skills, deep market insight and independence to help clients make sound decisions. The firm provides expertise in the areas of valuation, transactions, financial restructuring, alternative assets, disputes and taxation. With more than 1,000 employees, Duff & Phelps serves clients from offices in North America, Europe and Asia.

http://www.duffandphelps.com


cyber
gates

COMPUTER FORENSICS IN RUSSIA

Practical Aspects For Data Collection

by Roman Gorban

It is hard to imagine that time will pass and the use of hard copy documents will be perceived as something unusual and old-fashioned. At least this is true for Russia. Even though Russian legislation has made considerable progress in recognising electronic documents, it is rare to find a court where they have been treated as valid evidence.

WHAT YOU SHOULD LEARN

- In this article you will learn about certain areas of Russian Data Protection Legislation. You will also learn approaches commonly used in Russia to collect electronic evidence.
- You will also know how to handle electronic evidence, maintain chain of custody documentation, and also precaution measures that should be taken on forensic data collections in Russia.

It is hard to imagine that time will pass and the use of hard copy documents will be perceived as something unusual and old-fashioned. At least this is true for Russia. Even though Russian legislation has made considerable progress in recognising electronic documents, it is rare to find a court where they have been treated as valid evidence. For instance, Federal Law No. 63-FZ dated 6 April 2011 "On Electronic Signatures" defines the sphere of use of simple and certified electronic signatures. The Law regulates inter alia such areas as the acceptance of agreements placed on web sites (including agreements on terms of use), the use of logins and passwords and/or e-mail as a simple electronic signature, and also various confidentiality issues. In reality, however, although legislation is moving in the right direction, practical application of the law is not always possible. Russian lawyers and court officials are often reluctant to accept electronic documents and e-mails on the same basis as paper-based documents.

Is there any way to resolve this situation? Luckily, there is. First of all, a forensic practitioner should maintain a chain of custody records. In other words, the gathering, storage and processing of information should be documented at every stage. The guidelines for keeping track of evidence are more or less identical: an examiner needs to duly maintain transfer deeds (,) each time that evidence is received and released. Imaging forms also constitute an essential part of the chain of custody documentation. They should contain information on the source and target equipment used for imaging, the venue, date and time, unique hardware identifiers (S/N, part numbers, etc.), the names of the custodian and examiner. It is convenient and also frequently necessary to keep up-to-date notes in a deal book while acquiring the data. The records should allow for the reproduction of each step that has been undertaken, thereby providing the necessary level of defence of captured evidence.

However, what makes the whole process unique? Let's start from the very beginning. Before we take custody of a laptop, we need to carefully consider hidden pitfalls in Russian legislation. While the imaging procedure is transparent in some European countries and in the USA, the situation is different in Russia, which has complex and protective legislation on per-

sonal data. Now let's have a look at the definitions in Federal Law No. 152-FZ On Personal Data (as amended 25 June 2012). (:)

Which states that any information related to an individual and other data that can be used to identify an individual should be treated as personal data. This information includes:

- First name, patronymic and surname of the individual;
- Date and place of birth of the individual;
- Address, marital, property and social status, professional occupation and income;
- Other information about the individual defined in Federal Law No. 152-FZ (Clause 3).

One question comes to mind – what happens if one laptop at a corporation does not have such information on its hard drive? Even if there is such a laptop, how can we prove that this information is missing to a custodian? Is there a one-stop solution to gather information from a hard drive in a forensically sound way, leaving all personal and other sensitive information aside? What are the implications if the Law on Personal Data is breached? Will the examiner and examinee change places if something goes wrong?

Most lawyers will not provide you with definite answers to any of these questions. However, there is a way to mitigate the risks. A forensic examiner needs to study the employment contract and any policies that a custodian signed during the term of employment with the company. It is also advisable to take legal advice before collecting the data. A consent form authorised by the custodian could possibly be one of the most effective solutions. What about the contents of the consent form? It should have clear definitions of the employer, operators, documents, personal data and processing. The form should also contain all the permissions required for the gathering, processing, cross-border transfer and disclosure of personal data to third parties. It should contain the purposes of the processing and legal names of all the parties that gain access to the information, and also stipulate the terms under which the consent could be revoked. Such a consent form should be signed by the custodian… However, what should you do if the custodian refuses to sign such a form or there is a need to capture the evidence covertly?

There is a solution. The custodian's employer can provide a letter that guarantees, to the best of their knowledge, that no sensitive information can be found on the custodian's hard drive, including personal data, state or trade secrets and other prohibited content.

While hard drive images have been successfully collected, will electronic files extracted from them be accepted in a Russian court? It is highly likely that the answer would be NO. One way of generating electronic documents for a court is to print and notarize them. However, what should you do if the evidence needs to be supported by an expert witness? Are there any special qualifications in Russia that make the life of a computer forensic examiner even more complicated? The good news is that the requirements are fairly lax. For instance, according to Clause 13 of the Russian Federal Law on the "State Forensic Practice in the Russian Federation", the position of forensic expert can be held by a Russian citizen, who has a higher professional degree and subsequent training as an expert specialising in a particular area.

What if a considerable amount of data is collected in Russia for the purposes of foreign litigation. (?) What happens if the data should be shipped abroad? The cross-border transfer of information is permitted if the custodian has provided explicit consent and the country of destination has an adequate level of protection of personal data. Most European countries that ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Union Directive) can be considered as acceptable for data export, while the USA may not.

What other issues should also be considered before sending images from Russia abroad? If the data should be sent over the Internet, the transmitting and receiving parties should apply an encryption solution certified by the Federal Security Service of Russia (FSB) during the transmission of data over insecure channels of communication, as stated in Federal Law No. 152-FZ. Alternatively (,) the data may be shipped on hard drives or other electronic media. This media should not contain means of data encryption, while the data can be encrypted. The parties involved in the cross-border transfer of data should bear in mind that the Russian customs authorities might want to inspect the encrypted container thanks in no small part to the declaration of the goods containing a description of the transferred media

Are there any alternatives? Yes. It might not appear obvious at first glance, but the best way to transfer data from Russia is to keep the information in Russia. As Russian legislation is quite stringent in respect of personal data operators, the best way to secure and process the data is to select a local company that specialises in computer forensics. The company should have all the necessary tools and mechanisms for acquiring, storing and processing the data, and also an industry-level e-Discovery solution. The e-Discovery platform should make it possible to establish secure remote connections and should be capable of generating the requisite documents for the court. Such an approach helps to mitigate the risk that the data could leave the legal field, which would render further legitimate use of such information impossible.

Author bio

Roman Gorban, Senior Manager, Forensic Technology

Roman joined Forensic in 2006 after 3,5 years spent at KPMG in Markets and IT departments. He established the Ftech group and supported development of forensic services. Focusing mainly on Computer Forensics, he took part in international assignments which took place in Finland, UK and Ukraine.

Roman has a substantial experience in Cyber Forensics and was involved in a number of Fraud Investigation and AML projects in CIS, as well as conducted Forensic Technology work for KPMG member firms in Western Europe, UAE and US.

Roman is a public speaker at forensic conferences and is quoted in Russian media.

CLOUD FORENSICS AS A NEW TECHNOLOGY

by Shahrzad Zargari, David Benford

Cloud Computing is becoming so popular among organizations, promising simplicity and delivering utilities based on virtualization technologies. Convenience, availability, elasticity, large storage capacity, speed, scalability, and on-demand network access are some of the attractions of the cloud computing. The adoption of cloud computing solution is increasing rapidly which makes it inevitable for digital forensics not to follow since major potential security risks are surrounded this new technology. This study provides an overview of cloud forensics including the issues and the existing challenges in order to give better future prospects and also offers some steps to be taken to overcome these challenges.

WHAT YOU SHOULD KNOW

- Just a basic knowledge about digital forensics

WHAT YOU SHOULD LEARN

- The application of digital forensic in cloud computing and challenges for digital forensics investigators

INTRODUCTION

Cloud computing is a new buzz promising to provide simplicity and delivering utilities based on virtualization technologies. It provides availability, convenience, elasticity, large storage capacity, scalability, speed, and on-demand network access to a shared pool of configurable computing resources while charging the consumer based on the usage (pay-as-you-go), (Mell &Grance, 2011).

Although, this new technology provides many advantages, but the surrounding security issues are causing for concerns where some of these issues can be listed as follows: the location of data, the ownership of data, access control, regulatory requirements, liability and accountability in a case of security breach, investigative support, long term viability of the provider, data segregation, and disaster recovery and continuity plans, (Gregg, 2010).

The accessibility of multiple data storage around the world built by the cloud venders while they are shared and exchanged can lead to the loss of security controls over the cloud hosted on third-party cloud computing platforms.

The fast adoption of cloud computing solutions among organizations forces digital forensics to follow in order to tackle the aroused challenges.

DIGITAL FORENSICS: EVIDENCE AND PROCEDURE

Digital forensics is a process of analysing digital data while preserving its integrity. It includes the collection and preservation of sized media at the crime scene, validation, analysis, interpretation, documentation and presentation in a non-technical manner.

A complete documentation of the whole process of forensics investigation must be provided from the seizure of the digital equipment to the last phase of presentation of the evidence in order to maintain the chain of custody and satisfy the ACPO guidelines, (ACPO. 2009). In the cloud this process faces many challenges such as having limitations on the controls over the digital evidence. Digital evidence is any information of probative value which is stored or transmitted in a digital form based on SWGDE[1] definition which presents many challenges due to its characteristics. The quantity of potential evidence, easily contamination, the number of suspects, authenticity and integrity, reliability, completeness, admissibility, and juries' convincement are some of these challenges, (Reilly et al., 2010). Digital forensic procedure acquires precision and detailed documentation which includes five main steps as follows: Identification, Preservation, Collection, Examination, and Presentation to the court. In the cloud, each step involves new challenges which acquire careful consideration. For instance, in Identification phase, determining the location of data in the cloud, number of replica, ownership of the data, stability of the data, and limitation of triage techniques are some of the existing challenges for digital forensic investigation in the cloud.

CLOUD COMPUTING SECURITY ISSUES

There are potential security threats associated with the fact that data in the cloud are stored and processed remotely and also, the usage of virtualization and sharing of platforms between consumers which make the ownership boundaries of digital items blurry. Chow et al. (2009), presented a possible list of security threats in the cloud indicating that the traditional threats still exist in the cloud however they are more pronounced such as SQL-injection in platform level, phishing cloud provider, and expanded network attack surface. Jamil and Zaki (2011) published another list of threats in the cloud such as the loss of governance, lock-in, data protection and insecure or incomplete data deletion. The loss of governance applies when there is a gap of commitment between cloud providers and Service Level Agreement (SLA). In the cloud, often, there is a chain of dependency between cloud providers where sometimes causes difficulty in data portability within the cloud, being referred as lock-in. In addition to the above, the malicious insider could cause a major threat when one virtual machine attacks another which is difficult to detect.

There is no doubt that the cloud is a great technology which presents IT organizations with a fundamentally different model of operation however, due to its architect in a case of security breach, the major concern is the safety of the stored data. The location of data in the cloud is unknown which could be a disadvantage of the cloud computing. Even if one is able to determine the physical location of the server, it is difficult to find the precise data location on the server as each server is shared by numerous organizations. Another issue with the location of stored data is related to the jurisdiction that the data is stored in which can cause limitation for digital forensic investigation.

CLOUD FORENSICS

The application of digital forensic in the cloud computing environment can introduce a new term as cloud forensics. Cloud forensics can be a combination of traditional digital forensics and network forensics. There are different areas in cloud forensics that should be concentrated such as technical, structural, and legal aspects. The technical challenges in the cloud are occurred mostly in the process of data preparation and acquisition. Similar to online investigations, there is a potential risk of data loss during the imaging process for different reasons such as a virtualized server shuts down causing parallel or unrelated services to be interrupted. One of other issues in the cloud is the lack of access to main components such as network routers, load balancers, large firewall, and other networking components. It is a challenge to access the cloud application logs due to the nature of cloud such as multi-sharing resources, multi-jurisdictions, and being highly volatile and inconsistent. Moreover, the deleted data can easily be overwritten in the cloud thus; the investigator would not be able to recover the files in time. Investigations in hypervisor -levels can also be challenging especially if there is an insider threat.

In order to develop tools and procedures to carry out the digital forensics process in the cloud, some main keys should be considered.

- Forensics data acquisition: There are different cloud services and deployment models available in the cloud in which the process of identifying, labelling, recording and extracting data varies from one to another. This also includes whether the investigation is being carried out from client side or cloud service provider side.

- Elasticity of forensic techniques: It is essential for cloud forensics tools to be elastic in order to complete with rapid elasticity of the cloud. Large scale static and live forensic tools are required to deal with most cases such as e-discovery, data acquisition, data recovery, and evidence analysis tools.

- Investigation in virtualized environments: tools and procedures are required to be developed for investigations in virtualized environments such as hypervisor investigations and evidence retrieval from physical locations of data at a given timestamp.

- Evidence segregation: Cloud forensics involves the reverse process of evidence segregation from various shared resources in multi-tenant environment but the underlying cloud infrastructural components such as CPU caches and Graphic Processing Unit (GPU) were not designed for strong compartmentalization in a multi-tenant architecture. Therefore, it is necessary to develop tools and procedures in order to be able to segregate evidence among multiple tenants in different deployment models with different service models in the cloud.

- Proactive measures: Steps should be taken to facilitate the forensic investigation such as designing forensics-aware cloud applications and tools which proactively collect forensics data in the cloud, and conduct regular snapshots to remote storage, (CSA, 2011).

1. Scientific Working Group Digital Evidence < *http://www.swgde.org*>

The main challenge to forensic investigation in the cloud is the scope and diversity of operations in the cloud environment. Some of the research challenges can be named as follows: discovery of computational structure, attribution of data, semantic integrity, stability of evidence, presentation and visualization of evidence, and cross-jurisdictional aspects.
There is no fool-proof method of acquiring data forensically in the cloud which requires a combination of computer forensics and network forensics. The active data can be collected by traditional forensic tools, while its integrity is preserved, and for additional data over the network such as activity logs, network forensics tools are used. Activity logs can cause authentication issues due to being highly volatile, being overwritten, (Verma, 2011). E-discovery can be useful in cloud computing which refers to any process in which electronic data are sought, located, secured, with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or performed on a network, e.g. Encase have launched their own version however; avoidance of multi-jurisdictions problem is a major concern, (Biggs & Vidalis, 2009).
Encase and FTK have developed the ability of investigation in the cloud however, their tools are not sufficient. An open source tool was developed by a team from Stanford University in 2011 (https://bitbucket.org/Elie/owade/wiki/Home) which is claimed to be able to extract information form cloud services that a user accessed in his computer, reconstruct Internet activities and search for the online identities that were used. One of OWADE advantages is its ability to decrypt files ciphered using various Microsoft built-in encryption schemes and it combines this ability with traditional data extracting techniques in order to access Skype chat history, decrypt Internet Explorer stored logins and passwords, by cracking the windows user password, or access historical Wi-Fi location data stored by windows, delivering a list of access points with dates and times, (Bursztein, 2011).
It is difficult to reconstruct cloud services data stored in a hard disk since Windows scatters everything across multiple files and encrypts some portions whereas OWADE only searches, decrypts and puts together all of the cloud personal accounts, logs, logins and passwords that have been accessed, (Bursztein, 2011). OWADE (Alpha version) is still being developed and at the moment it only works in Windows computers.
Some of the most useful information in digital forensics is within the logs files which can also assist the application developers for fault monitoring, assessing feature usage, and monitoring business process. There are challenges associated with cloud-based log analysis and forensic such as, decentralization of logs, volatility of logs, multiple tiers and layers, archival and retention, accessibility of logs, non-existence of logs, non-compatible or random log formats, and absence of critical information in logs, (Marty, 2011). In the cloud, logs are stored on multiple servers and in multiple log files by a cloud -based application. Logs files have volatile nature and only are available for a certain period of time. Therefore, Marty (2011) proposed a set of practical guidelines instrumented in application to address the existing challenges within log files. These guidelines explained different situations such as when there is a need to log, what sort of information need to be logged, or how to log them. However, the paper only explained briefly the implementation of these guidelines in SaaS for Django, JavaScript, Apache, and MySQL.
The structural aspects of cloud forensics should involve the consumer and the cloud provider. A list of required parties to be involved in the cloud forensics can be listed as follows: investigators, IT professionals, incident handlers, legal advisors, and external assistance in case of performing forensics tasks such as e-discovery.
It is important to mention that cloud providers and most cloud applications often have dependencies on other cloud providers therefore an investigation may depends on one of the links in the chain and level of complexity of the dependencies. Essential communications and collaborations through this chain need to be facilitated by organizational policies and Service Level Agreements. The chain of cloud provider and consumer also has to communicate and collaborate with law enforcement, third parties, and academia in order to facilitate effective and efficient forensic activities, (Ruan et al., 2001).
The legal aspects of cloud forensics are related to the challenges of investigations in the multi-tenancies and multi-jurisdictions. These are the major legal concerns in digital forensics where regulations and agreements have to be developed to secure the forensic actives not to breach any laws or regulations.
Legal considerations should also be focused on the Service Level Agreements which is the terms of use between the consumer and the cloud provider. In order to facilitate forensic investigations, SLAs is required to include extra terms as follows:

- Service provided, techniques supported, and access granted by cloud provider to the consumer regarding forensic investigation
- Trust boundaries, roles and responsibilities between cloud provider and consumer
- The protection of forensic investigations in a multi-jurisdictional environment in terms of legal regulations, confidentiality of consumer data, and privacy policies (Ruan et al., 2011).

CLOUD FORENSICS FOR DIFFERENT MODELS

Data centralization in the cloud would be a benefit to forensics investigation which leads to a faster coordinated response to incidents and also a dedicated ready to use forensic server. The high availability computer intense resources and potentially peta-bytes of storage are some of the advantages of cloud computing related to digital forensic. Moreover, inbuilt hash authentication for authentication of disk images shortens the time consumption of generating MD5 checksums. However, the main issues are still remaining for the digital investigations in the cloud such as remote datacentres, evidence authenticity and integrity, securing and evaluating the scene, documenting the scene, RAM acquisition, and deleted data recovery.

INFRASTRUCTURE AS A SERVICE (IAAS)

In IaaS, the consumer has the administrative access, so it can deploy virtual machines where in some cases (GoGrid), the VMs use persistent storage (bits would be written to the disk if a VM is rebooted). The advantages are the ability to perform deep interrogation of the machine, so traditional forensics can be used. And also many of IaaS providers support snap-shooting a running VM, therefore, the state of a running host can be captured quickly (via API that shoots a host after system monitoring detects anomaly). The disadvantage is that a robust connectivity to the Internet should be present.

PLATFORM AS A SERVICE (PAAS)

The consumer deploys application packages to a runtime environment that is hosted by a cloud provider so the consumer owns the core application, and programmatically dictates how it would interact with other dependencies. The advantage is the core application is controlled by the organization therefore, log information can be customized in a way that by invoking the custom code, the system state can be interrogated and logs be pulled. The disadvantage is that the provider may confine the access to logging information.

SERVICE AS A SERVICE (SAAS)

In SaaS, the provider invokes an instance of an application and the consumer can apply basic configurations or may be able to interface with the application via an API, however, no deep programmatic control are involved in order to modify the core application of the system. The advantage is that high level application logs might be available either success logs and failure logs, or the actual activities within the environment which it depends on the provider decision. Many providers of messaging solutions in the SaaS email deployment have an option for "message journaling" which tells the provider to transparently forward a "carbon-copy" of all messages to archive service, (Birk, 2011).

CRIMEWARE-AS-A-SERVICE

CA Technologies (Internet security business unit) reported that an emerging trend is now happening towards the creation of Crimeware-as-a-Service with almost all Trojans (96%) developed as a result of this tactic. It also claimed that cyber criminals are increasingly reliant on cloud-based web services and applications, such as Google Apps, Flickr and Microsoft Office Live, as well as real-time mobile web services to target general users. The criminal have already started to develop exploit kit such as Incognito which is web-based application represented as MaaS (Malware as a Service), and it is located in the cloud providing services to underground communities, (Bruke & Baving, 2011). Cloud computing could still suffer from traditional attacks such as DDoS, attacks targeting parts or the entire cloud. In addition, a cloud can be used as a tool to conduct or plan a crime and attack other cloud.

CLOUD FORENSICS IN MOBILES

Most of the existing mobile applications use cloud computing such as Facebook and Google Mail. Based on Gartner prediction, 90% of companies will support corporate applications on personal mobile devices by 2014 therefore, if a company has very little control over its mobile phones, therefore any misuse may be difficult to be traced. The full impact of cloud computing on the digital forensic community is yet unknown, (Biggs and Vidalis, 2009), thus, mobile forensic will be suffering if research does not start developing cloud-based mobile forensic in terms of tools, methodologies and procedures. Mobile commerce is a new innovation which is causing a concern in digital forensic community. For instance, wave and pay is a new method of payment where no longer consumers need to pay by bank card and the bill will automatically be paid with a swipe of a mobile.

In 2011, Zhu carried out a research to find out whether the existing forensic tools are able to extract all the information within smartphone devices. Different digital forensic tools (e.g. XRY v5.5 & Oxygen) were used as well as the open source tools. Zhu findings indicated that the current forensic tools and methodologies could not extract data from cloud storage based applications such as Dropbox and also have difficulties extracting cloud based emails such as G-mail. Cloud based emails can only be extracted if the phone is jail-broken or has a root access right however, the cloud service provider would be able to collect the emails where the integrity of the data would not be 100%, (Zhu, 2011).

CONCLUSIONS

Cloud computing is an emerging computing paradigm aiming to share storage, services, computation where is pushing digital forensics to new limits. Cloud computing delivers its low cost services through the use of large data centres for storage in different jurisdictions with multi-tenant hosting by virtual servers. These are the factors that make challenges for digital forensics since the location of data and its replicas (for backup reasons) are unknown. Plus these data are stored in different jurisdictions where different legislations regarding the data access may have been applied and also the ownership of these data is in question due to sharing the resources (multi-tenancy). The traditional digital forensics is not able to compete with cloud technology therefore cloud forensics as a new term was defined (Ruan et al., 2011) as a cross-discipline between cloud computing and digital forensics which also is a subset of network forensics, including three dimensions of technical, organizational, and legal dimensions. Opportunities and Challenges in each dimension were discussed in order to overcome the difficulties in the forensics investigation procedures in cloud computing, the following steps are recommended by this work.

- Reconstructing the ACPO guidelines for cloud forensics. This will protect the digital forensics investigators from dealing with legal issues while providing them with some reliable procedures and regulations to follow in order to maintain the chain of custody
- Revising regulations and laws regarding the digital forensics investigations in cloud computing
- The development of Forensics as a Service in cloud computing (by cloud developers) in order to employ fast and reliable procedures for investigations according to ACPO guideline
- Revising the Service Level Agreement in a committee including a representative of consumers, cloud providers, digital forensics experts, and legal advisors. SLA should be written in a way that assists digital forensic investigators while there is no breach of privacy or regulations
- Attempts should be made to regulate internationally the use of cloud computing services therefore; the forensic investigators have less limitation in different jurisdictions (towards harmonization).
- Research must be conducted to develop new cloud-based forensics tools to effectively and efficiently facilitate the forensic investigations.

Authors: Shahrzad Zargari & David Benford;
University of Derby

REFERENCES

ACPO,"Good Practice Guide for Computer-Based Electronic Evidence", online available < http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf>

Biggs S., Vidalis S., "Cloud Computing: The Impact on Digital Forensic Investigations", The Institute of Electrical and Electronics Engineers, IEEE press, 2009

Birk D., "Technical Challenges of Forensic Investigations in Cloud Computing Environments", 2011, [Online] available < http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf>

Burke W., Baving R., "Cyber Forensics in the Cloud: Challenges and Best Practice", Sequirt CSi BV, 2011, [Online] available < http://www.hackerhalted.com/Portals/3/Docs/Presentation%20Slides/Cyber-Forensic-in-The-Cloud-day3-Wayne-Burke.pdf>

Bursztein E., Fontarensky I., Martin M., and Picod J.,"Doing Forensics in the Cloud Age OWADE: Beyond Files Recovery Forensic", 2011, online available < http://cdn.ly.tl/talks/owade-paper.pdf>

Carmenatty E., "Cloud Computing a Forensics Immature Technology", A Unit of Knowledge (KNOL), July 2010, online available < http://knol.google.com/k/cloud-computing-a-forensics-inmature-technology#>

Chow R. el at., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", Proceedings of the 2009 ACM workshop on Cloud Computing Security, ACM, 2009, online also available < http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html>

Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0", 2011, Online available <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf >

Delport W., Olivier M., and Kohn M, "Isolating a Cloud for a Digital Forensic Investigation", Information and Computer Security Architectures Research Group, Dept. of Computer Science, University of Pretoria, South Africa, August 2011, [Online] available < http://icsa.cs.up.ac.za/issa/2011/Proceedings/Research/Delport_Olivier_Kohn.pdf>

Emma Webb Hobson, "Cloud Forensics-Lab Systems' Solutions", Senior Digital Forensic Investigator, QinetiQ, 2010 online available < http://www.labsystems.co.in/images/Cloud_Forensics_-_A_Lab_systems_approach.pdf>

Fu X., Ling Z., Yu W., and Luo J., "Cyber Crime Scene Investigations (C2SI) through Cloud Computing", Int. Con. On Distributed Computing Systems Workshops, IEEE press, pp. 26-31, 2010

Gregg Michael, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Online available < http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_VI_10SecurityConcernsCloudComputing.pdf >

Houmansadr A., Zonouz S., and Berthier R., "A Cloud-Based Intrusion Detection and Response System for Mobile Phones", IEEE press, pp. 31-32, 2011

Ieong Ricci, "Challenges to Digital Forensics from Cloud Computing", eWalker Consulting Limited, 2011, [Online] available < http://www.china-forensic.com/downloads/2011/CCFC-2011-ISFS-Ricci-Presentation-E.pdf>

Jamil D., Zaki H., "Cloud Computing Security", Int. Journal of Eng. Sc. and Tech (IJEST), vol. 3, pp. 3478-3483, 2011 Online available < http://www.ijest.info/docs/IJEST11-03-04-129.pdf>

Lawton George, "Cloud Computing Crime Poses Unique Forensics Challenges", 2011, Online available <http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges>

Lee J., Hong D., "Pervasive Forensic Analysis based on Mobile Cloud Computing", Electronics and Telecommunications Research Institute (ETRI), IEEE press, pp.572-576, 2011

Lu R., Lin X., Liang X., & Shem X., "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proceedings of the 5th ACM (ASIACCS)'10, pp. 282-292, 2010, [Online] available < http://bbcr.uwaterloo.ca/~rxlu/paper/asiaccs185-lu.pdf>

Marty Raffael, "Cloud Application Logging for Forensics", IEEE Press, 2011, online available < http://loggly.com/assets/4de13091dabe9d0c7800005f/applicationlogging.pdf>

Mell P., Grance T., "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, NIST, U.S Department of Commerce,2009 Online available <www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>

Podhradsky A., Casey C., "Digital Forensic Challenges in a Cloud Computing Environment", 2011, Online available http://searchcloudsecurity.techtarget.com/tip/Digital-forensic-challenges-in-a-cloud-computing-environment>

Popovic K., Hocenski Z., "Cloud Computing Security Issues and Challenges", IEEE Press, MIPRO 2010, Opatija, Croatia, pp. 345-349, 2010

Reilly D., Wren C., Berry T., "Cloud Computing: Forensic Challenges for Law Enforcement", Internet Technology and Secured Transactions (ICITST), IEEE Press, London, 2010

Ruan K., Carthy J., Kechadi T., Crosbie M., "Cloud forensics: An Overview", Centre for Cybercrime Investigation, University College Dublin, 2011, online available < http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf>

Ruan K., Baggili I., Carthy J., Kechadi T., "Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary analysis", University College Dublin, Zayed University, 2011, Online available < http://www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf>

Verma Pankaj, "The challenges of Cloud Forensics", 2011, online available < http://blog.lighthousedt.com/?p=408>

Wolthusen Stephen, "Overcast: Forensic Discovery in Cloud Environment", Norwegian Information Security Laboratory, IEEE press, pp. 3-9, 2009

Zhu Meng, "Mobile Cloud Computing: Implications to Smartphone Forensic Procedures and Methodologies", MSc Thesis, Auckland University of Technology, 2011 [Online] available < http://aut.researchgateway.ac.nz/bitstream/handle/10292/2660/ZhuM.pdf?sequence=3>

Author bio

Dr Zargari studied Forensics Computing and Security at the University of Derby, and has published at peer-reviewed international conferences in applied statistics, digital forensics and network security. She is an experienced researcher who has been involved with IT industry for more than 15 years. Shahrzad has developed a passion for digital forensic and network Security. In the last few years, she has employed her background knowledge in applied statistics to computer security. At the moment, her research topics involve cloud forensics, data mining, cybercrime, and network security.

Audiobook

PRODUCTION

Published Forensics Author?

If you are, and your book has not been narrated and professionally produced as an Audiobook for Audibles.com, then you are overlooking one of today's most rapidly growing markets.

The Audiobook industry serves as a powerful tool to both authors and their readers who are too busy to flip pages.

We're pursuing 100 Authors for publication.

We provide public relations and marketing support by transforming you into a public relations savvy "Subject Matter Expert".

If your topic is training friendly, all the better, we produce training materials and videos as well.

Legacy Strategic Development, LLC
www.legacy-strategic-development.com
1- 718-285-7962 | Brooklyn, New York, USA

HOW SECURE IS MY REMOTE CONNECTION?

by Paul Gafa

This article will guide you through the settings available to configure your remote connection in a secure way.

WHAT YOU SHOULD KNOW

You must have previous experience with „Remote Desktop Connection" and preferably „Microsoft Terminal Services" or cloud computing in general

WHAT YOU SHOULD LEARN

How can we ensure that we have the correct settings in place and how can we get the most secure connection

Remote Desktop Connection to your Windows machine has been available for quite a long time. Over the years the Remote Desktop Protocol (RDP) has evolved to provide higher security and better performance. Nowadays, due to users' mobility, access to remote desktops or access from the cloud is very common. If you need to access important data while travelling, remoting to your desktop is a better solution than actually carrying the data with you, as no data is lost if your device is lost or stolen. How can we ensure that we have the correct settings in place and how can we have the securest connection?

HISTORY

The first operating system which supported RDP protocol was NT 4.0 which was released in 1996. The RDP version used was also 4.0. The latest Windows Operating Systems - Windows Server 2012 and Windows 8.0 - include the latest version which incidentally is also version 8.0. In 16 years security has always been of interest and we will see what we can do to get the most out of the system in this regard.

SECURITY WITH SERVER SESSIONS

Microsoft RDP Protocol comes with a few options which will determine the Security Level and Encryption used during a session. These options are pretty easy to set if you are connecting to a server by opening the Remote Desktop Session Host Configuration Management Console Snap In. Choose the General category as shown in Figure 1.

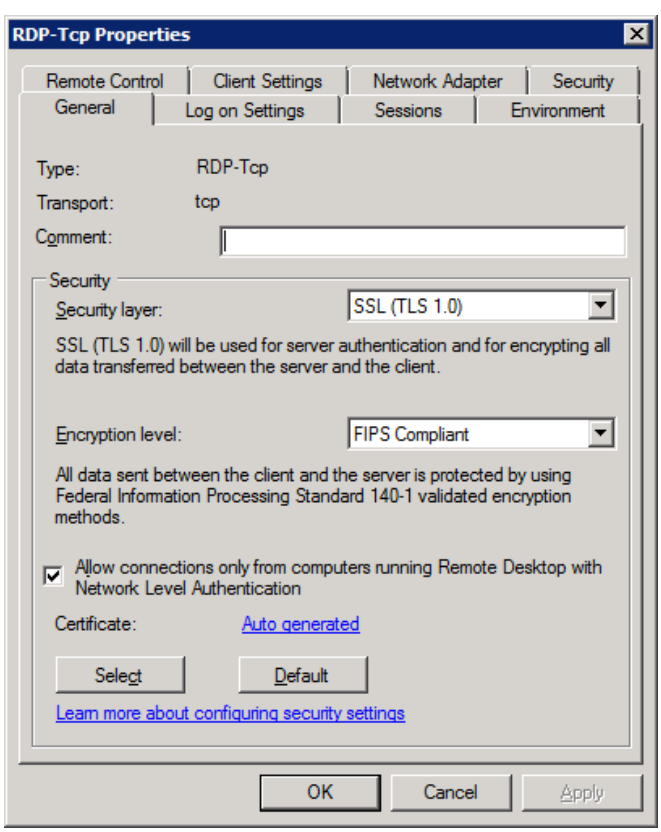


Figure 1. The RDP security options on a Windows 2008 R2 Server

The Security Layer can be set to RDP Security Layer, SSL (TLS 1.0), or Negotiable where the best available option is used. It is advisable that whenever possible SSL is used. When SSL is in place the client can verify that it is actually connecting to the correct server by validating the server certificate. You need to ensure that the certificate used was issued by one of the trusted Certification Authorities.

The client has the following options to validate the server certificate:

- If server authentication fails, connect to the computer without warning **(Connect and don't warn me)**
- If server authentication fails, do not establish a connection **(Do not connect).**
- If server authentication fails, show a warning and allow me to connect or refuse the connection **(Warn me).**

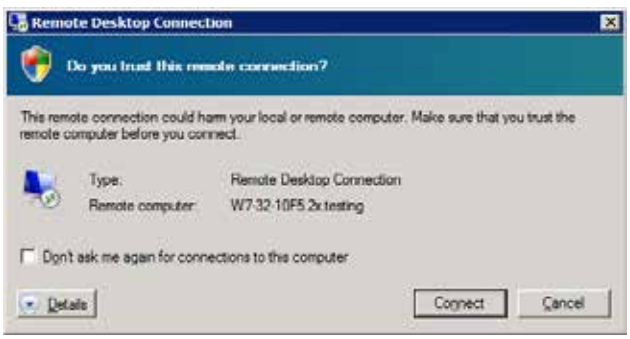


Figure 2. Client connection warning for a certificate which is not trusted

If the client is connected using an SSL connection a lock icon is shown on the connection bar when the session is in full screen mode as shown in Figure 3.

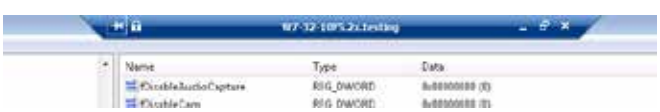


Figure 3. Lock icon shown on the connection bar.

When RDP encryption is used, you can select the Encryption Level which can be set to one of the following:

Low	All data sent from the client to the server is protected by encryption based on the maximum key strength supported by the client.
Client Compatible	All data sent between the client and the server is protected by encryption based on the maximum key strength supported by the client.
High	All data sent between the client and the server is protected by encryption based on the maximum key strength of the server. Clients that do not support this key strength are not allowed to connect.
FIPS Compliant	All data sent between the client and the server is protected by using Federal Information Processing Standard 140-1 validated encryption methods. Client that does not support FIPS are not allowed to connect.

When SSL is used you can opt to enable "Network Level Authentication". This means that the user is authenticated before the Remote Desktop Session is created making access more difficult for potential attackers. This means that if authentication fails, the user will not be able to enter his credentials at the Windows login screen as the connection will be terminated. Limited resources from the server are used unless the user is actually authenticated, reducing the risk of Denial Of Service attacks. If the client in use does not offer _____

SECURITY WITH WORKSTATIONS SESSIONS

If a workstation is joined with a domain these settings can be pushed via group policies.
The policy path is: **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security** as shown in Figure 4.

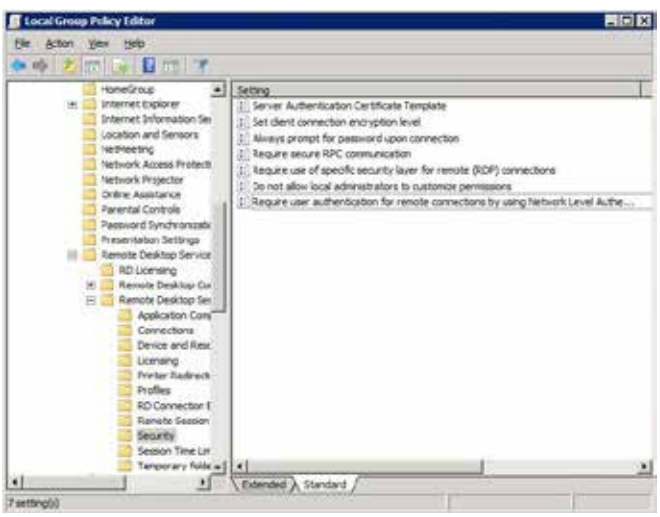


Figure 4. Security Group Policy

However if the workstation is not joined to a domain we need to be able to change these settings directly from the registry. Windows XP, Windows Vista, Windows 7 and Windows 8 do not offer a user interface to configure all these settings. You need to modify the registry settings at:

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER\WINSTATIONS\RDP-TCP

As always, back up your registry settings before you make any changes.
To modify the Security Layer you need to set the entry SecurityLayer. Possible values are as follows:

0	Communication between the server and the client will use native RDP encryption.
1	The most secure layer that is supported by the client will be used. If supported, SSL (TLS 1.0) will be used.
2	SSL (TLS 1.0) will be used for server authentication as well as for encrypting all data transferred between the server and the client. This setting requires the server to have an SSL compatible certificate. This setting is not compatible with a MinEncryptionLevel value of 1.

To modify the Encryption Level you need to set the entry MinEncryptionLevel as follows:

1	Low level of encryption. Only data sent from the client to the server is encrypted using 56-bit encryption. Note that data sent from the server to the client is not encrypted.
2	Client-compatible level of encryption. All data sent from client to server and from server to client is encrypted at the maximum key strength supported by the client.
3	High level of encryption. All data sent from client to server and from server to client is encrypted using strong 128-bit encryption. Clients that do not support this level of encryption cannot connect.
4	FIPS-compliant encryption. All data sent from client to server and from server to client is encrypted and decrypted with the Federal Information Processing Standard (FIPS) encryption algorithms using the Microsoft cryptographic modules. FIPS is a standard entitled „Security Requirements for Cryptographic Modules". FIPS 140-1 (1994) and FIPS 140-2 (2001) describe government requirements for hardware and software cryptographic modules used within the U.S. government. Clients that do not support FIPS are not allowed to connect.

HOW CAN I MODIFY MY CONNECTION TO ACHIEVE A HIGHER LEVEL OF SECURITY?

Since RDP protocol is well known it is not a difficult task to find public servers and attack them. It is advisable to protect your server from being discovered as an RDP enabled machine.

The most obvious thing to do is change the port on which the service is running but there are more advanced ways to protect your server.

CHANGING THE DEFAULT PORT

By default the RDP port is set to 3389, thus anyone wanting to attack your machine is likely to force an attack on this port. You can easily change this port by following these simple instructions:

1. Start Registry Editor.

2. Locate and then click the following registry subkey:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber

3. On the Edit menu, click Modify, and then click Decimal.

4. Type the new port number, and then click OK.

5. Quit Registry Editor.

6. Restart the computer.

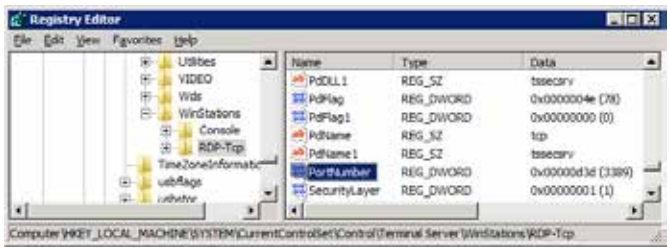


Figure 5. Changing the RDP default port

If your machine is behind a router you may only need to change the port forwarding rule on your router.

DIFFERENT RDP CLIENTS AVAILABLE

Microsoft distributed various RDP Clients with their operating systems. Depending from which version you are running you may not have access to the latest features in security.
It is important that the RDP version is Version 6.0 or higher in order to be able to use Network level Authentication. RDP clients running version less than 5.2 do not support TLS. Other third parties RDP clients may lack one or the other feature.

VPN, SSL OR SSH TUNNELS

An easy way to hide your RDP enabled machine is to put the listening port behind a VPN, SSL or SSH tunnel, so that before the user can connect to the RDP protocol he must first open the VPN, SSL or SSH tunnel. If this requires authentication then the security level within RDP is protected by the tunnel. There are various products on the market which are able to do so. A typical setup is shown in figure 6. The client connects to a gateway which has only port 443 (SSL) enabled. Thus a potential attacker is not aware of the services that lie behind the gateway. The gateway will authenticate the user before it forwards the connection to the destination server.

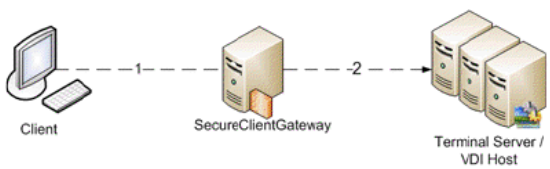


Figure 6. Remote Desktop Servers behind an SSL enabled gateway.

SECOND LEVEL AUTHENTICATION

Some products add an extra level of security by introducing a second level of authentication. This can be an RSA key token or simply a request for a One Time Password, sent via SMS or email when needed. Another form is a software version of a key token which can be installed on your smart phone or machine. Products can verify the device from which you are connecting and warn the user if the connection is made from a new device.

DO NOT KEEP THE DEFAULT REDIRECTION SETTINGS

If you allow other users to connect to your machine or if you might connect from a public machine it is advisable to not allow files to be copied from the client to the server machine. This will protect the host from being infected with unwanted applications. The clipboard may also be a source of unwanted

data on your machine so disabling the redirection of 'Drive' and 'Clipboard' makes your system safer. Allowing redirection of 'Plug and Play' devices may result in installation of new drivers on your system, so it is advisable to keep this feature disabled in order to further stabilise your system, as redirection is normally not needed.

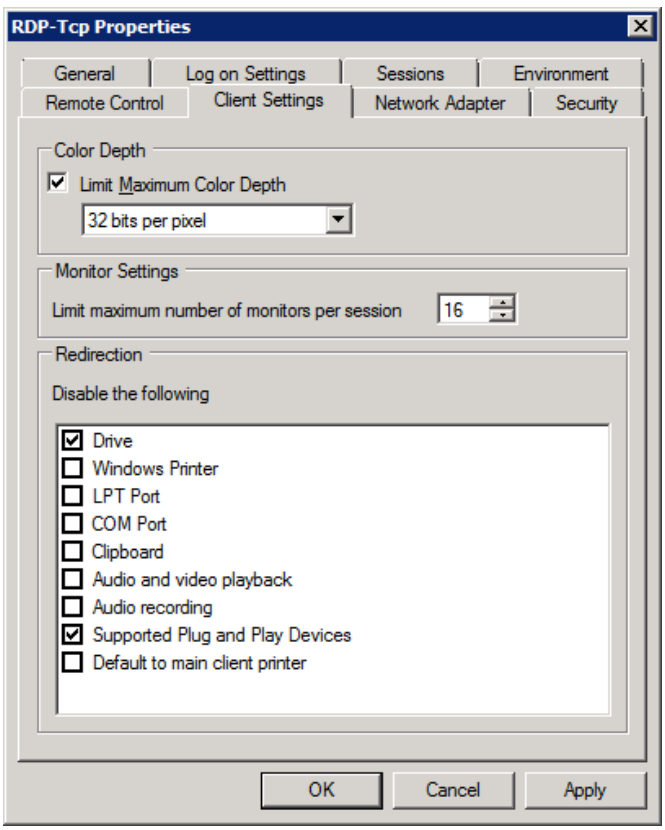


Figure 7. Redirection settings in the Remote Desktop Host Configuration

PERFORMANCE

Adding more security does not decrease the quality of the user experience. With the improvements made in the last version (7.0 - 8.0), the Remote Desktop Protocol provides excellent user experience both on a LAN and on a WAN. Accelerated multimedia now make it possible to stream high quality media.

KEEP YOUR MIND AT REST

Security has always been one of the areas in which Microsoft have invested so as to improve their system. We have seen various settings which can be used to secure your connection. Unfortunately some of the options are only available in the latest versions of the Windows operating system. Using a third party application to SSL tunnel your session will protect your RDP session irrespective of the version of RDP. If you can control which devices access your machine(s) and receive alerts if someone who is not authorised is trying to gain access, you can keep your mind at rest!

Author bio

Paul Gafa'Position: CTO for 2X Software Ltd
I have been working in the IT industry for the last 21 years.
I specialize in communication protocols main focus being cloud computing and server based computing.
I am responsible for the technical decisions taken at 2X Software.
I love to design and implement network protocols.
In my career I have developed projects for all the major operating systems with preference to low level real time applications.
Projects I worked on range from Connection Broker to various Hyper-visors, Secure Client Gateways, Terminal Servers Load Balancer, Remote Desktop Clients, X11 Servers, Network File System Servers, X11 to RDP Gateways, Terminal Emulators,

THE CCTV FILE FORMAT MINEFIELD

by Dr Mark Sugrue

The first and often most difficult issue faced by CCTV investigators is simply getting the video evidence to play, but tips and technology can help…

WHAT YOU SHOULD KNOW

- With 3000+ video file formats in the CCTV industry, viewing footage can be a challenge.

LEARN HOW TO

- Identify formats and the best places for get 3rd party player applications.

CCTV footage is a rapidly growing source of evidence for Law enforcement agencies. It has surpassed fingerprints and other common evidence sources. The growth in CCTV as a source of evidence has primarily arisen due to a fundamental shift in technology– the move from Analog to Digital surveillance systems. Whilst the technology shift has provided a rich source of evidence, there are some technical issues which can give Law enforcement agencies a headache.

Digital Video Recorders began to replace older Analog CCTV recorders about 15 years ago, and they promised a lot: better quality, ease of use and reliability. One important feature was lost in the changeover: a standard data format.

With Digital Video Recorders it was left to the manufacture to decide how to actually encode and store the video data. With no proper industry standard to follow, each manufacturer brewed their own file format, and made players to accommodate the format. The result is near chaos.

We at Kinesense have documented more than 1,500 different CCTV video file formats in circulation. This is by no means all the formats that exist, and DVR manufacturers (mainly Chinese and South Korean companies) are producing new formats on a weekly basis. Our best estimate is that there are a minimum of 2,500 to 3,000 file formats and codecs in existence.

When an investigating officer is handed a disk or USB key containing case-critical CCTV video, he usually needs to first try to identify the file format and spend hours trawling the internet and specialist forums trying to locate the right player software. It is a very time consuming, inefficient process and has huge knock on costs through the whole law enforcement system.

HISTORY: HOW DID WE END UP WITH THIS MESS?

The first widely adopted digital video file format was Microsoft's 'AVI' format, released with Windows 3.1 in 1992. AVI is a versatile, and therein lies the problem for CCTV. AVI is a container format; meaning it has a standard file header, but the actual data can be encoded in any way desired. All that's needed is a codec – a small piece of software installed and hidden away on your PC that does the work of decoding the file. The AVI file header contains a four letter code which describes which codec is used, so then Media Player runs off to the Registry, finds the codec software, and plays the file. Great, in theory…

The problem is that 1992 was long before the modern internet. The four character identifier in the AVI header isn't enough to tell the computer where to get the codec if it doesn't happen to be installed already. A four character code (formally called

'FourCC') could be unique – there are over 16 million possible combinations – however, Microsoft never thought to include any way of issuing unique codes or of preventing companies from using a few popular codes. (Actually, this isn't quite fair. Microsoft does ask that manufacturers email them to register new FourCC codes, but there doesn't seem to be any place to look up the full official list; neither does there seem to be any enforcement) There are 835 different AVI codecs in our format database with many companies using the same four characters to represent different codecs.

Figure 1. Privately operated CCTV can be quite poorly maintained.

AVI is only the beginning of this story. There are at least 20 different 'open' video file formats – meaning the layout of the file is publicly available. A few of these are used by DVRs. Flash (flv) and mpg (and its evil twin, VOB) are used by a few manufacturers. Of the open formats, AVI is the most common in CCTV, and within AVI, most manufactures use their own, non-standard, codecs.

That brings us to the nest of vipers that are closed video file formats. Most DVR manufacturers don't even adhere to the loose and flexible AVI standard. They branch out all on their own and make something completely new – and completely incompatible with everyone's format or player. This isn't just a minor irritation – there are now thousands of incompatible and undocumented video formats in circulation, and it is increasingly difficult to simply identify the brand or origin of a video file.

THE COST OF CCTV

CCTV is a powerful tool and, when a crime is caught on camera (and the video quality is good) few other types of evidence are as convincing to a judge or jury. The cost of gathering CCTV evidence is monumental. The UK has one of the highest densities of CCTV cameras of any major country, with an estimated 5 million CCTV cameras – the vast majority of which are privately owned and operated. Other countries may have fewer cameras, but are catching up quickly. A Study by Tayside Police in Scotland has shown that at least 65% of criminal investigations gather CCTV evidence, and a similar study by Cheshire police showed that 75% of that is from 3rd party sources. This means that half of all criminal cases involve video evidence captured from private DVRs (which equates to approximately 900,000 cases in the UK each year).

What is the cost of this to the police? There is no systematic study which quantifies the cost in time or resources of finding and recording or copying CCTV, bringing back to the station or delivering it to the audio-visual department, or even the cost in time and manpower of simply watching it – but that cost must be vast. I have spoken with quite a number of UK bobbies who find that their routine police work is frequently sidetracked by hours spent fiddling with DVRs and attempting to play or retrieve the footage, or simply driving the possibly-important but unplayable video recording in a squad car to the Audio-visual department. The number I have heard anecdotally is an average of two hours per week, per officer. That equates to 5% of each police officer's time, or about 13 million man-hours per year across all 43 UK police forces. This calculation does not include the knock on costs and delays to the back office and technical staff or to case preparation or to the courts.

Figure 2. "Have you seen this man?" Badly installed CCTV can be next to useless, as in this image released by Blackpool Police in August 2012. http://www.blackpoolgazette.co.uk/news/cctv-plea-over-attack-at-club-1-4818286

CCTV need not be this inefficient. DVRs could be designed with standard formats and user interfaces. Technology does exist to speed up the process of accessing video, of sending it securely (without having to use a squad car!) to a server and for speedily reviewing it. In many forces, audio-visual or computer crime departments end up doing too much of the work that should be done by investigative officers and there are tools available to enable front line officers to do this work.

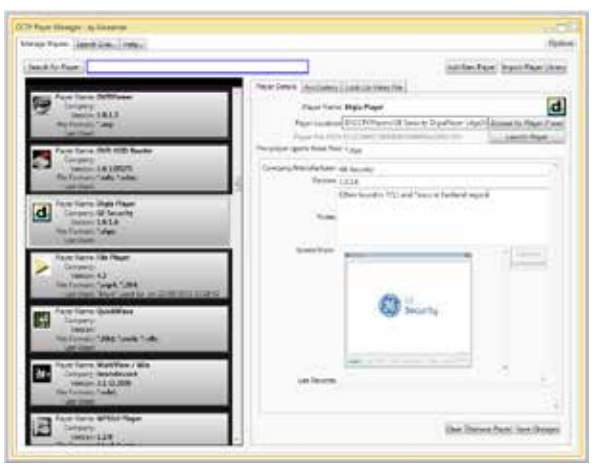


Figure 3. Player Manager with a list of players, screenshots and searchable notes on each one.

CCTV VIDEO FILES: HOW TO VIEW THEM?

So what can be done when faced with a new and unknown video file from a CCTV DVR? There are a number of tools and clues that can help identify it.

- **Which file is the video file?**

  An investigator is typically presented with a CD/DVD or USB key with video evidence. Determining which file on the device is the video file should be straightforward but often it is not. When video is retrieved from the DVR, lots of random log files can also be exported along with the important video files. Sometimes the data arrives in a complex folder

tree with the important video files squirreled away up in the high branches of the folder structure. Generally, the video files will be the largest files on the disk. The tool TreeSize Free is handy for quickly scanning the size of folders and subfolders and detecting where the big files are.

- **Can the DVR supply the player software?**

  Sometimes, kind and considerate DVR manufactures configure their machines to save a copy of the CCTV player to the disk or USB key when you hit 'export'. Sometimes, this is an option hidden away in a menu. If the DVR can give you the player or codec, perfect. More often than not, the DVR doesn't do this.

- **What is the file extension of the video file?**

  The letters or numbers after the final '.' in the video file name are key to identifying it. If the file ends in 'AVI' the next step is to determine what codec the file requires. If it is 'mpeg', 'mpg', 'flv' or one of the other open formats, the file will likely play in a standard movie player such as VLC or Windows Media Player. If it is none of these, the file format is most likely closed and will only play in the manufacturers own software.

- **Identify t he AVI Codec?**

  For AVI files, the codec is written into the file header. It is possible to look yourself by opening the file in HxD (look at byte position 188) but two fine tools exist to make this easier: MediaInfo and GSpot. Either tool will give you useful information, such as width, height and duration; but the key information is the codec. Maybe 850 different AVI codecs exist. If you find the right one, download it from the manufacturer, and install it correctly, then Windows Media Player should play the file.

  Useful sites for finding information on codecs are fourcc.org, Vid-ID.com and media-geek.com (more about these below).

- **Identify a proprietary CCTV file format?**

  This one is tough. There are at least 1,500 to 2,000 different proprietary (closed) video file formats in use. If MediaInfo can't open it, and VLC or Windows Media Player can't play it, most likely the file is simply a closed format that can only play in the player software supplied by the DVR manufacturer. There are a few websites that can help identify the format and suggest players to download.

  Kinesense's own Vid-ID tool is a good place to start. Just open the website *www.Vid-ID.com* and select the file you wish to identify. Vid-ID checks its internal database of file formats and emails a list of possible matches to you. For AVI files, you should use the Media-Info application to access the codec name, and then enter that into Vid-ID.

  Kinesense also make a handy desktop application called Player Manager which includes an off-line copy of the Vid-ID database and can automatically detect the codec name in AVI files and tell you which codecs are already installed on your PC. It does more than this – it also searches your hard disk to find CCTV players and tells you which one to use for a given file. Player Manager keeps notes on each player, can record tips on how to use it and keep screenshots. When you encounter a new file, and download a new player, it becomes part of the Player Manager database. Player Manager can back up your library of players and let you synchronise the library across different PCs. You can download a free 30 day trial of Player Manager from the Kinesense website.

  Alternatively, there are a number of websites which offer long lists of file formats where you can manually look up a file type. Most of these sites are members only, or restricted to police in particular countries.

  Media-geek.com is certainly one of the best collections of format and player information available, and includes a wiki with reams of useful information. It is members only, but membership is free of charge and open to forensic investigators in any country.

  The London Metropolitan Police have an online DVR and codec database but it is restricted to UK Police only. CCTV-codec.com is a similar site based in Denmark. In the next few months, the FBI is planning to launch their own codec database. This one will be freely accessible to everyone I am told, and will be found at: www.fbivipr.org.

MOST DIFFICULT FORMATS

The player applications themselves can be quite a pain, even after you have found a match for that troublesome format. Some players have not been updated in years and only work in XP, Windows 2000 or even earlier incarnations. This is where keeping detailed notes on how to use each player, and sharing this information across the police force reaps rewards.
Kinesense's own Vid-ID.com tool gives us a unique insight into which video formats investigators find the most troubling. The online tool is used by thousands of investigators around the world. For all those overworked forensic investigators facing the latest frustrating DVR or video format, rest assured you are not alone – this is a problem shared by police in at least 112 different countries. Google Analytics provides a breakdown of country of origin for (anonymised) website visitors. Visitors from the UK top the poll for using Vid-ID, followed by the US, India, Canada, Japan and, somewhat surprisingly, Trinidad and Tobago! The most searched for formats are .box (used by i3DVR and SAY Security), .bix, .dat, .264 – I interpret these as being the most perplexing formats, rather than the most common.

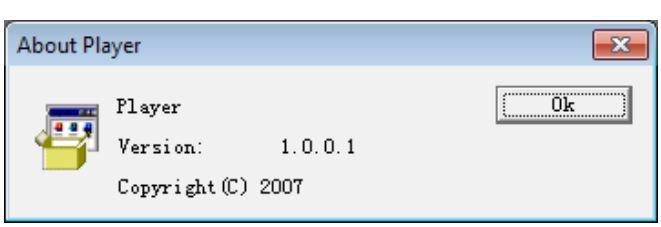


Figure 4. An 'About Box' from a player called 'Player', providing very little useful information.

THE FUTURE

The chief driver of CCTV installations is not government or police, but insurance companies, who offer sizable discounts to clients with CCTV cameras. Strangely, insurance companies don't specify a minimum level of quality – meaning the only pressure on the CCTV owner is cost, and they will almost

always buy the cheapest DVR which allows them to claim the insurance discount. The owner buys, installs the system, and then forgets about it until some incident occurs. The true end user is the police who are faced with badly maintained cameras, old DVRs, lost manuals and forgotten passwords. CCTV can often be of such poor quality as to be useless as evidence. Even so, police must spend the time to collect and view this video before they can determine if it is usable.

What is needed is a proper industry standard which specifies a common file format and a minimum level of quality. There is work being done both in the US and EU to write such standards, but they are years away and actual enforcement seems unlikely to be stringent. Even when such a standard is in place, it will be many years, if not decades, before all the older non-standard DVRs are replaced. Again, only the insurance companies truly have the clout to set and enforce such a standard – but while the true end user – the police – continue to shoulder the cost of the current system, neither the insurance companies nor their customers are likely to change.

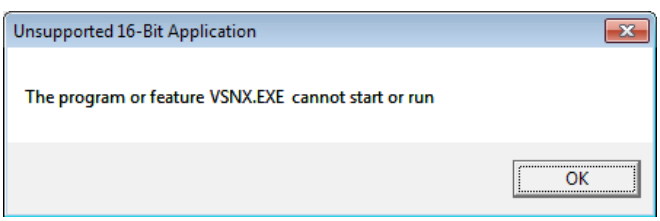


Figure 5. This error message suggests this CCTV player was designed for Windows 3.1, pre-1995. The DVR is still in use.

Despite all this, CCTV can be an excellent source of evidence and it will continue to be used. During this time of tightening police budgets, some modest changes to work practices and adoption of new technology with regards to the collection and reviewing of CCTV presents considerable opportunity for savings.

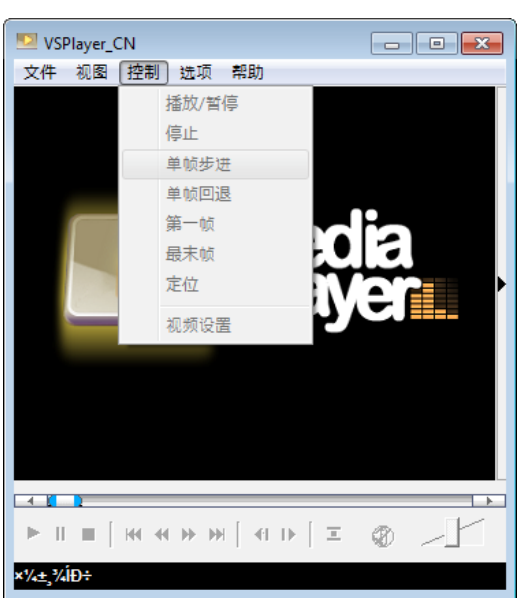


Figure 6. Many player applications are difficult to use so keeping good notes on how to use players is essential.

USEFUL LINKS

- www.media-geek.com website by LEVA member Larry A. Compton for the Forensic Multimedia Community.
- www.Vid-ID.com A free tool for finding codec and format information
- http://www.headbands.com/gspot/ G-Spot Codec Information Appliance software
- http://mediainfo.sourceforge.net/en MediaInfo tool for identifying codecs
- http://www.kinesense-vca.com/product/kinesense-player-manager/ Kinesense Player Manager
- http://www.jam-software.com/treesize_free/ TreeSize Free – for scanning folder sizes
- http://mh-nexus.de/en/hxd/ HxD – for looking at file bytes
- http://fbivipr.org/ A FBI DVR database (in development).
- http://cctvcodec.com/ A members only codec database based in Denmark
- http://www.videolan.org/vlc/index.html VLC player by VideoLan
- http://www.fourcc.org/ More information on FourCC codes
- http://www.doktorjon.co.uk/ CCTV News site

Author bio

Dr Mark Sugrue is Chief Technology Officer of the Video Analytics company Kinesense Ltd and is responsible for new product development. He holds a BSc in Applied Physics from the University of Limerick and a PhD in Video Analytics from the Royal Holloway, University of London. Kinesense has worked with law enforcement and security agencies in Europe and North America for many years and is focused on making CCTV more efficient and easier to use for the police. Kinesense products and services include the video search and reporting products “Kinesense Law Enforcement” and “CovertSuite”, the free Vid-ID.com tool and Player Manager.

IN THE UPCOMING ISSUE OF EFORENSICS NETWORK...

WIRELESS FORENSICS

& MORE...

Available to download on November 10th

If you would like to contact eForensics team, just send an email to en@eforensicsmag.com. We will reply a.s.a.p.

2X ApplicationServer XG

Virtual Desktop & Application Delivery

Simple and secure virtual desktop & application delivery to any mobile or desktop device.

2X ApplicationServer screen

Publish Applications and Desktops

Universal Printing

Automatic Redundancy

Web Portal

2X Software Ltd HQ
109, 4th Floor
Sir William Reid Street
Gzira GZR 1033
Malta

Tel: +356 22 583 800
Fax: +356 21 311 841
Support: support@2x.com
Sales: sales@2x.com
Website: http://www.2x.com/

COMPUTER FORENSIC & DATA RECOVERY

The evidence your case needs is most likely on someone's computer or network.

Chartstone analysts will determine the evidence location and format to collect, preserve, analyze and present it.

You can be confident in Chartstone. We only use proven, trusted, industry-leading forensic solutions and methodologies. Chartstone analysts have years of experience with civil and criminal cases including:

- Unauthorized disclosure of corporate or trade secret data
- Employee internet / computer / email abuse
- Employee termination
- Criminal fraud / deception
- Harassment
- Divorce
- And more…

Chartstone will recover data from:

E-mail
Webmail
Smartphones
Documents
Images and video
Internet artifacts

Deleted files
Backup files
Encrypted files
Workstations
Servers
RAIDs

Web history and cache
Chat sessions
Compressed files
Disk or RAM
Tablets
And more….

INFORMATION SECURITY SERVICES

Chartstone will provide guidance and practical solutions to protect and secure your information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Our services include:

Training and Awareness
Social Engineering Testing
Enterprise Risk Management
Policy and Procedure Assessment and Development

Vulnerability Assessment
Penetration Testing
Disaster Recovery and Business Continuity
Regulatory Compliance

Chartstone
Digital Forensic and Information Security Services

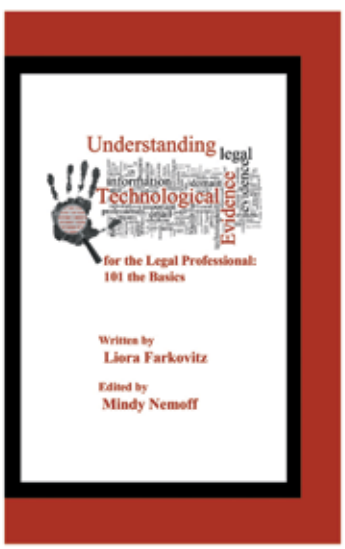
www.Chartstone.com

203-233-3523
Info@Chartstone.com

www.TechnologicalEvidence.com
USA 1.718.285.7962

Come on, admit it, when you talk, their eyes just glaze over. So tell them,

We make it so easy!



Our 92 Page Tech Guide Free when they buy The Electronic Advantage: 101 The Basics

4 Hours, Online, Novice Friendly, Informative, Refreshingly Pain Free!
10 Case Examples

Only $360.00 USD

Because "justice" is not a joke, it's our responsibility.

Promoting Forensic Technology Literacy
TechnologicalEvidence.com a project of
Legacy Strategic Development, LLC
Brooklyn, New York USA

Liora Farkovitz

Forensic Author Publishing

Live or Online Training & Materials

Training Videos

Technical Guides

Forensic Technology Syndicated Broadcasts