

(IN) SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 38 - June 2013

WHAT STARTUPS CAN LEARN FROM
ENTERPRISE LEVEL DATA SECURITY TACTICS



UEFI SECURE BOOT
TO HACK BACK OR NOT TO HACK BACK?
IT SECURITY JOBS

Security in knowledge

Mastering data. Securing the world.



**Intensive information security.
Essential intelligence in just three days.**

Information security today isn't optional. It's business-critical. Over three days, RSA® Conference Europe 2013 imparts the must-know actions to manage growing cyber threats. With 70 sessions spanning 10 hours, attend the educational and networking event that builds your knowledge and furthers your career.

- Leave with actionable solutions
- Build your knowledge and skills
- Develop your professional contacts
- Stay informed, stay ahead

(IN)SECURE subscribers receive an extra €100 off. Use discount code 56E3HELPND when you register.

**Early Bird
discount,
register by
26th July**

**Hear how the world's security experts
manage challenges like:**

- Bring-Your-Own Device
- Cloud security
- Mobile and tablets
- Big Data
- Data breaches
- Hacktivism
- Cybercrime
- Malware threats

Find out more at:

www.rsaconference.com/help

TABLE OF CONTENTS

Page 05 - **Security world**

Page 11 - Becoming a computer forensic examiner

Page 15 - UEFI secure boot: Next generation booting or
a controversial debate

Page 20 - How to detect malicious network behavior

Page 23 - **Malware world**

Page 29 - What startups can learn from enterprise level
data security tactics

Page 33 - To hack back or not to hack back?

Page 36 - Report: Infosecurity Europe 2013

Page 38 - DNS attacks on the rise:
Rethink your security posture

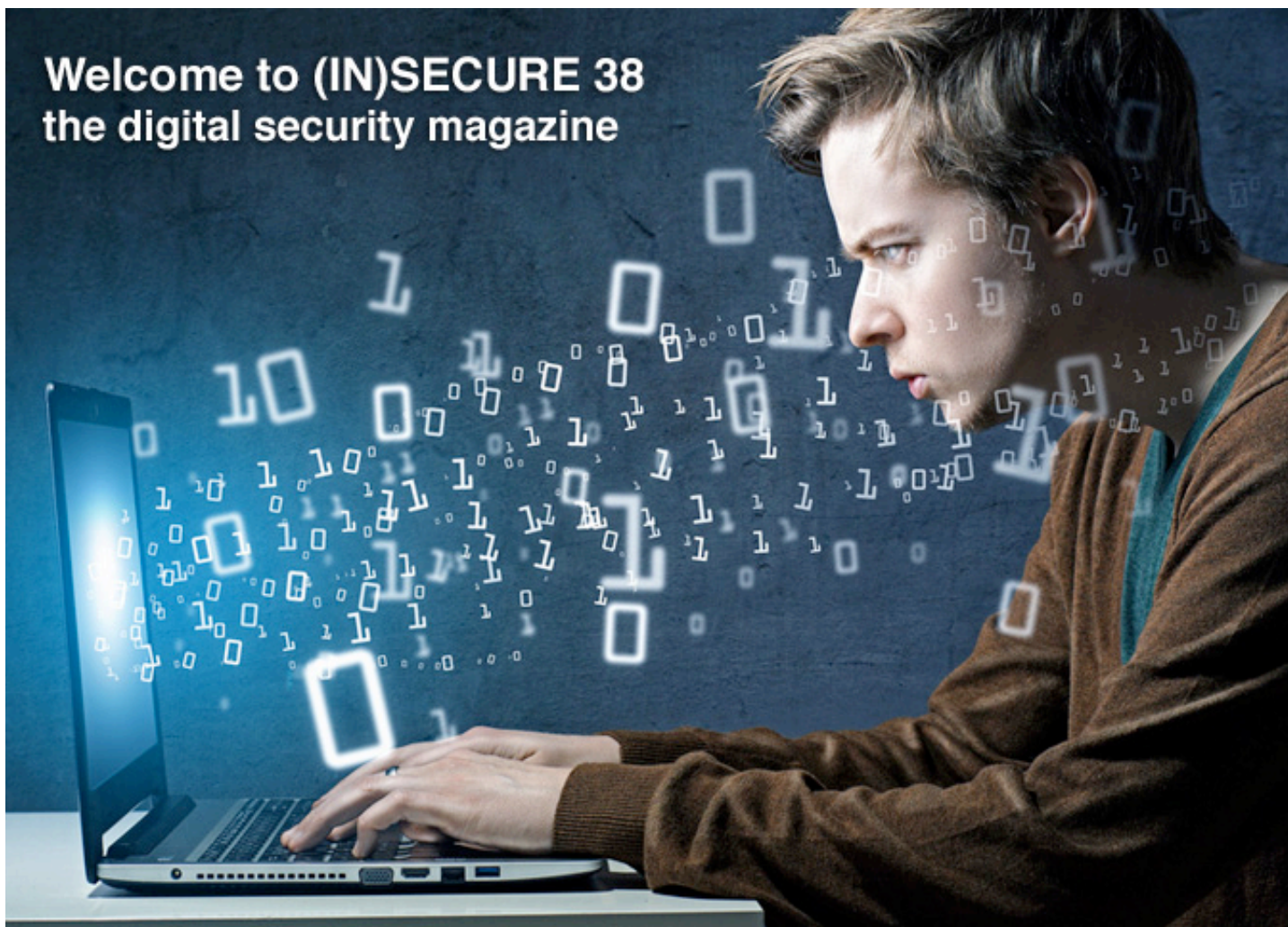
Page 41 - Events around the world

Page 43 - IT security jobs: What's in demand and
how to meet it

Page 46 - Remote support and security: What you don't
know can hurt you

Page 49 - A closer look at HITBSecConf 2013 Amsterdam

Welcome to (IN)SECURE 38 the digital security magazine



As much as I like going to industry conferences, enjoying their energy and frenzy, and getting together with old friends, sometimes company events like the BalaBit IT Security one I recently attended in Budapest inspire me even more. Getting to meet so many dedicated security experts and a peek into their everyday work really makes you conscious of the fact that we are all doing our best to "fight the good fight."

With that in mind, this is our latest contribution to it, and we hope you'll enjoy it.

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 - mzorz@net-security.org

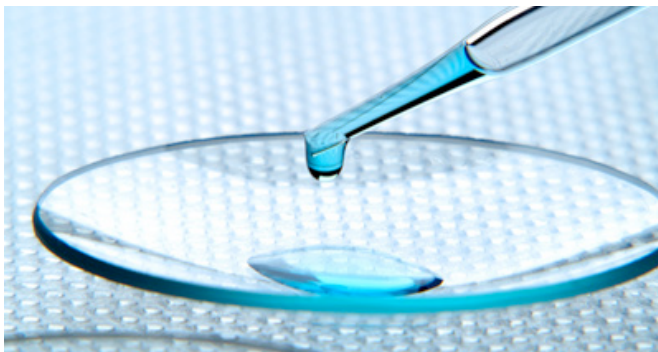
News: Zeljka Zorz, Managing Editor - zzorz@net-security.org

Marketing: Berislav Kucan, Director of Operations - bkucan@net-security.org

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.

Researches test resilience of P2P botnets



Following increased efforts by a number of companies and organizations, the takedown on botnet C&C servers is now a pretty regular occurrence and cyber crooks have reacted by decentralizing the communication between bots and their controllers.

They mostly opted for Peer-to-Peer (P2P) communication infrastructures, which made their botnets more difficult to disrupt.

Nevertheless, there are ways of doing it, and a group of researchers from the Institute for Internet Security in Germany, VU University of

Amsterdam, and tech companies Dell SecureWorks and CrowdStrike has decided to test botnets' resilience to new attacks.

While acknowledging that estimating a P2P botnet's size is difficult and that there is currently no systematic way to analyze their resilience against takedown attempts, they have nevertheless managed to apply their methods to real-world P2P botnets and come up with quality information.

They used crawling and sensor injection to detect the size of the botnets and discovered two things: that some botnets number over a million of bots, and that sensor injection offers more accurate results.

With their disruption attacks - sinkholing and partitioning - they have discovered that there are weaknesses which could be used to disrupt the Kelihos and ZeroAccess botnets, and that the Zeus and Sality botnets are highly resilient to sinkholing attacks, and say that research on alternative P2P botnet mitigation methods is urgently needed.

Changes to the Java security model



The most significant change is how signed applets are handled. In the past Oracle has suggested that all websites switch to signed applets, advice that contradicts recommendations by security experts, because

signing an applet would also confer privileges to escape the sandbox.

In fact, signed applets are the original method of escaping the Java sandbox, and have been abused by both attackers and security auditors for the last decade. Metasploit has a module specifically for this purpose. Oracle is changing this model so that signing an applet no longer confers sandbox escape privileges. This is a good thing for security.

The second change has to do with whether unsigned applets are allowed to run. In recent versions of Java, unsigned applets required additional steps on behalf of the user to run.

This change will make that even more cumbersome and push developers to always sign their applets, something many were loath to do with the existing security model. This change also allows the whitelisting of specific web sites and central management of Java security policies, something that has been a significant problem for enterprises so far.

The last change relates to certificate validation. In order to verify that an applet has a valid signature, Java needs to walk the certificate chain, making sure that it ends in a trusted root. This works fine until a certificate has been revoked due to a compromise.

Taken as a whole, this is good thing for Java, but these changes don't solve the underlying problem with the Java sandbox itself.

Internet-savvy Turkish protesters turn to anti-censorship apps



In the months leading up to the current protests in Turkey, its government has been censoring content on Twitter and Facebook, as well as throttling and blocking access to them, claim sources inside of the country.

After having successfully censored the majority of the television channels that can be seen in Turkey, the government is aiming its

sights against social networks again. The escalating protests have spurred the country's Prime Minister Recep Tayyip Erdogan to demonize Twitter and social media in general as a "menace to society."

Turkish Internet users are anticipating increased censorship and surveillance efforts by the government, and have begun arming themselves with tools to foil them.

Anchorfree, the makers of the Hotspot Shield mobile app that allows users to use an untappable virtual private network to connect to sites that are censored by the local government, have said that more than 120,000 users from Turkey have downloaded the app over the first weekend after the protests have started.

More and more users are turning to Twitter to get the latest news about the protests, and to apps such as Zello and Ustream to communicate in short distances and record and broadcast videos.

Windows 8.1 will allow locking folders with a finger

Windows 8.1 is scheduled to be released at the end of 2013, and among the various changes that Microsoft aims to implement in it is native support for fingerprint readers, so that fingerprint-based authentication becomes an integral part of the users' experience.

So far, Windows has been supporting fingerprint readers only via drivers and software offered by third parties. But, things are about to change as the company is working with PC and equipment manufacturers and is encouraging them to include fingerprint readers in mobile computers (laptops, tablets) as well as input

devices such as keyboards and computer mice.

Users of this Windows version will be able to use their fingerprints to seamlessly log into their computer, Microsoft account, apps, and sign off on online payments. They will also have the option of locking (and unlocking) private folders with it.



OWASP top 10 web application risks for 2013



OWASP has released its 2013 top 10 list of risks associated with the use of web applications in an enterprise, and they are as follows:

- 1) Injection
- 2) Broken Authentication and Session Management
- 3) Cross-Site Scripting (XSS)
- 4) Insecure Direct Object References
- 5) Security Misconfiguration
- 6) Sensitive Data Exposure
- 7) Missing Function Level Access Control
- 8) Cross-Site Request Forgery (CSRF)
- 9) Using Known Vulnerable Components
- 10) Unvalidated Redirects and Forwards.

Net neutrality soon to be on EU's agenda

Lack of regulation has contributed much to the success of the Internet, and made it a hotbed for new ideas. But there are some things that should be regulated and enforced in order for it to remain just that, and net neutrality is one of them, says the European Commissioner for Digital Agenda Neelie Kroes.

"The 2011 study by European regulators showed that, for many Europeans, online services are blocked or degraded – often without their knowledge. For around one in five fixed lines, and over one in three mobile users," she said on Tuesday while addressing at the European Parliament in Brussels. "It is obvious that this impacts consumers, but

start-ups also suffer. Because they lack certainty about whether their new bright ideas will get a fair chance to compete in the market."

Kroes shared that she will be putting forward proposals to the College of Commissioners, which will aim to assure that citizens get "the fairest deals, the most choice, the best new services over the fastest networks," keep the Internet open, and provide ISPs with incentives to improve the infrastructure.



Smart TVs vulnerable to a host of attacks

"Until now, most of the security researchers working with connected TVs focused on security vulnerabilities related to physical access to the device's USB port or local network access," AG researcher Martin Herfur pointed out, adding that a paper published by the researchers from German TU Darmstadt addressed mostly privacy-related issues with the HbbTV standard such as WiFi eavesdropping.



His own research and that of his collaborators demonstrated that content that is requested by the Smart TV at the time the user changes the channel can be altered by attackers, allowing them thusly to make the URLs within the DVB stream to point to servers with their (potentially malicious, or simply annoying) content.

Some TV stations that are using HbbTV are using poorly configured servers which can be compromised to serve malicious content, and they are not using SSL secured connections, which means that attackers can again lead users to malicious content by deploying a Man in the Middle attack.

Other attacks can lead into the TVs becoming roped into a Bitcoin mining botnet, users seeing fake news on the news ticker (the "moving stripe" on the screen that offers headlines and stock information), and being subjected to viewing unwanted content.

ISC-CERT warns about medical devices with hard-coded passwords

Approximately 300 different surgical and anesthesia devices, ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment have been found to have hard-coded passwords - a fact that can be taken advantage of by malicious actors to change devices' critical settings or even modify their firmware.

The discovery of this vulnerability has been made public by ICS-CERT and the U.S. Food and Drug Administration (FDA), both of whom issued alerts, but assured that there is no indication that such attacks have been already spotted in the wild.

They have, understandably, not shared the names of the manufacturers and the devices that have been found to be affected by the flaw.

In the meantime, healthcare facilities have been urged to evaluate their network security

and protect their hospital system by restricting unauthorized access to the network and networked medical devices, keeping antivirus software and firewalls up-to-date, monitoring network activity for unauthorized use, protecting individual network components through routine and periodic evaluation, developing and evaluating strategies to maintain critical functionality during adverse conditions, and contacting the specific device manufacturer if they think they may have a cybersecurity problem related to a medical device.



Changes to the standard for PIN Transaction Security



The PCI Security Standards Council published version 4.0 of the PIN Transaction Security Point of Interaction requirements. Changes:

Restructured Open Protocols Module – helps ensure POI

devices do not have communication vulnerabilities that can be remotely exploited to gain access to sensitive data or resources within the device.

Enhanced interface testing and logical security requirements – by requiring more

stringent documentation and assessment of all interfaces of the device, will help ensure that no interface can be abused or used as an attack vector.

Added source code reviews – additional mandatory source code reviews enhance the robustness of the testing process.

Introduction of a vendor provided security policy – provides guidance that will facilitate implementation of an approved POI device in a manner consistent with the POI requirements, including information on key management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.

Proposed bill will deny foreign hackers entry into the U.S.

The Cyber Economic Espionage Accountability Act, sponsored by Representatives Mike Rogers Tim Ryan and Senator Ron Johnson, "will give the President and Congress the power and oversight to deal with foreign cyber espionage in a meaningful way," claims Congressman Ryan.

"It's time there are repercussions for these brazen acts taken by foreign actors. This bill is a simple, common-sense measure. It directs the Administration to develop a list of cyber spies, make that list public, and enforce

penalties for those bad actors," commented Senator Johnson.

The bill is meant to encourage the DOJ to prosecute economic espionage criminal cases against offending foreign actors, to deny known or suspected foreign hackers visas and entry to the U.S.



Most enterprises have no information strategy



Less than 10% of today's enterprises have a true information strategy, according to Gartner. In order to break through to higher levels of corporate enlightenment on information centricity, here are three methods:

Visualize: Companies that find better ways to represent complex information will win in

better internal decision making capability and in better service products to their customers.

Vision and breakpoint: People are often much more willing to entertain big, challenging ideas if they seem to be a way off into the future – because they seem less threatening.

External exposure: Datasets buried in you own systems could be of far wider value and, if exposed, they are more likely to be linked together in new and innovative combinations that might create even more value.

How businesses prepare for disasters

With fears of potential security breaches and natural disasters weighing heavily on IT executives, businesses have continued to grow and advance their business continuity and disaster recovery plans to incorporate the adoption of wireless network capabilities, cloud services and mobile applications.

The annual AT&T Business Continuity Study found that:

- 87 percent of executives indicate their organizations have a business continuity plan in place in case of a disaster or threat – a slight uptick from last year (86%).
- 66 percent (two-thirds) of companies are using or considering using cloud services to augment their business continuity strategy.

- For disaster recovery purposes, a plurality of companies plan on leveraging cloud computing for data storage (49%).
- Three-fourths (78%) of companies indicated that their business continuity plan accommodates the possibility of a network security event.
- Seven out of ten (73%) companies are taking proactive or reactive measures to protect against DDoS attacks.
- The majority of organizations surveyed invest in mobile security services. Of those companies, 66 percent take proactive measures against DDoS attacks.



How organizations should handle personal data on IT systems that they don't control



Carsten Casper, research VP at Gartner, and proposes the following steps:

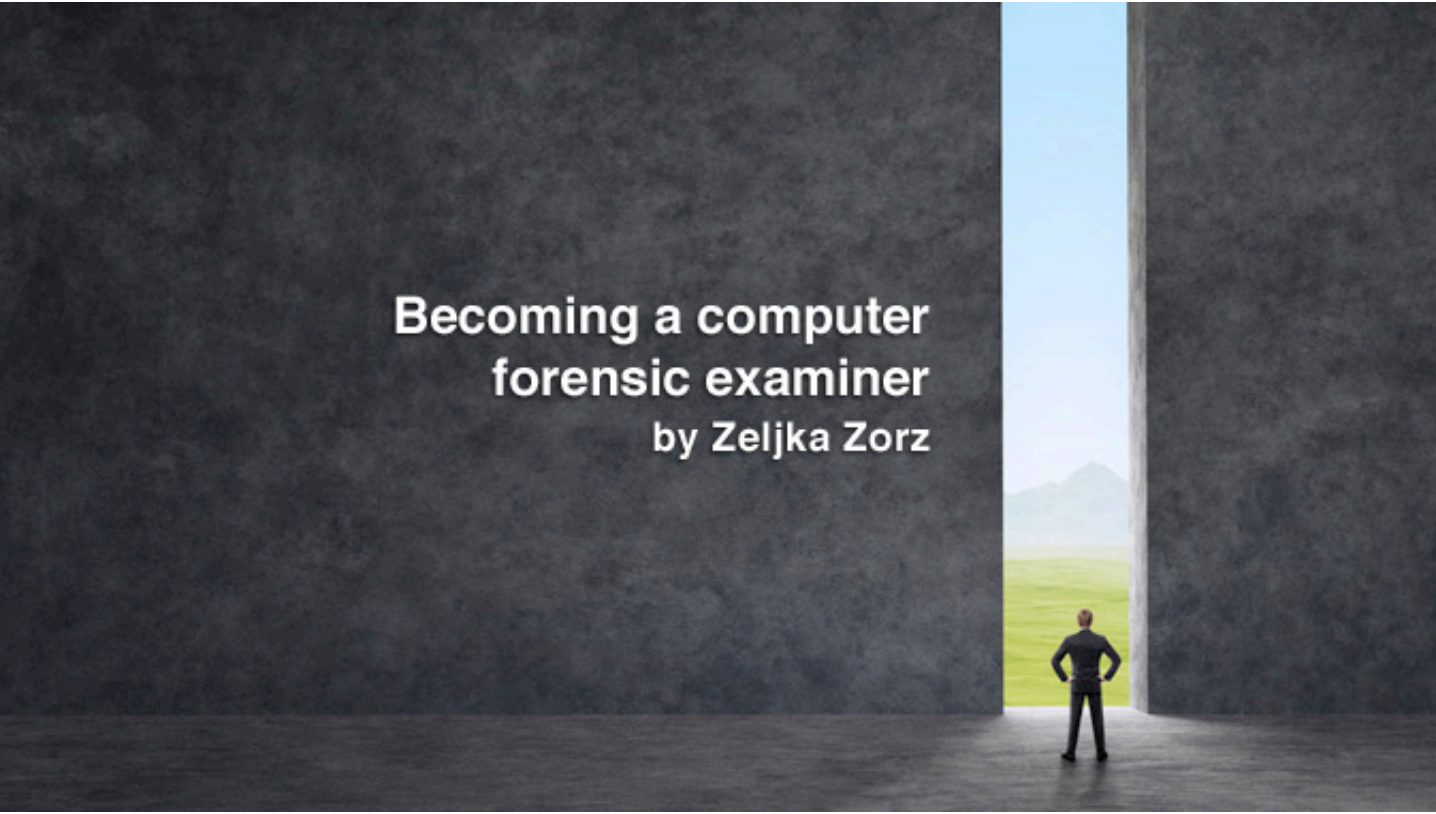
Create clear delineations between personal and nonpersonal data - The true challenge resides in handling data that can fall into both categories. Whether an organization decides for or against declaring certain types of data as "personal data" depends on the organization's risk appetite.

Put a fence around personal data - Encryption is the most widely used protective control. An additional challenge exists where the organization does not own the underlying IT infrastructure — be it a mobile device or a cloud environment.

Favor purpose-built over general-purpose applications - Any technology that processes personal data in the same way it processes nonpersonal data creates a risk.

Adhere to privacy standards, or create your own - Privacy standards simplify control frameworks, audits and information exchange, especially in scenarios where many players and stakeholders are involved.

Logical location rules over physical and legal location - If a data center of a U.S. cloud provider is operated by a third-party service provider from India, the data is encrypted, the Indian IT employees manage only routers and servers, and only European employees of the client can actually see the data, the data is logically in Europe.



Becoming a computer forensic examiner

by Zeljka Zorz

Since the advent of affordable personal computers, digital devices, and later the Internet, these technologies have been used for both legal and illegal purposes, and in order to collect evidence to help prosecute some of the people engaged in the latter, a new science had to be born: digital forensics.

One of the branches of digital forensic science is computer forensics, which deals with legal evidence that can be extracted from computers and digital storage media.

Evidence secured by practicing it has begun to be used in criminal law in the mid-1980s, and since then, the need for computer forensics and specialists that practice it has risen in concordance with the exponential escalation of computer and computer related crime.

But as Gary Kessler - president of Gary Kessler Associates, a consultancy that among other things offers services related to computer, network, and mobile device forensics - tells me, breaking into the field is surprising hard considering the need for this specialty.

"One key is that someone who wants to enter the field has to be prepared to move. While there are a ton of information security jobs and they're all over the place, computer forensics companies large enough to hire entry-level people or give internships tend to be clustered in the larger population centers," he points out, adding that the U.S. government

can also provide great training, and that the DoD and DHS are currently hiring.

"I would recommend you get at least a bachelor's degree in computer science so you have a good background. Get experience in a corporate IT department and then you can work for a law enforcement agency or cyber security firm, among others," advises Dr. Hans Henseler, founder of the Forensic Computer Investigation Department at the Netherlands Forensic Institute, and managing partner of the Forensics Business Unit at Fox-IT, the Dutch security audit firm that investigated the DigiNotar breach.

"Starting in law enforcement helps to obtain important experience and after five years you can go to a commercial company and be very valuable," he says, and points out that while many law enforcement agencies require one to be a law enforcement officer, some will hire civilians or outsource their work to commercial companies.

In the U.S. that could mean any number of federal, state, and local agencies, including

the FBI, secret service, IRS, SEC, Department of Justice, and so on. In the Netherlands there are perhaps twenty different government bodies involved in computer forensic investigations.

Kessler's advice on being prepared to move might even mean moving around the world. According to Henseler, there is a big need for people in Asia, including China and Singapore.

"If you take advantage of these opportunities you can grow your career quite fast," he says, adding that being able to speak several foreign languages as well as to communicate well with non-technical staff such as lawyers and accountants is a big plus.

Maqsood Ahmed, Principal Security Consultant (EMEA & APAC) at Guidance Software got his start in the British Police Force, in 2002, with one of United Kingdom's biggest ever computer crime investigation. "I've always been interested in IT and so Operation Ore, coupled with my IT skills, was a right fit."

"I enjoy the digital analysis and the development of technology, various processes, procedures, and so on. I don't necessarily consider it a difficult job – more of a hobby," he adds, then points out that a good computer forensic investigator has to be inquisitive, analytical, detailed and have an advanced level of interest in technology.

"I think the recipe for success is a mix of higher education and professional certificates, coupled with common sense, as well as professional certificates that can demonstrate your interest in, and ability to understand the security field, technology, processes, and so on."

If you're wondering where to get the needed education, Henseler offers some pointers: "We are starting to see Bachelor and Master programs in Computer Forensics offered. For example, the University College in Dublin offers a masters degree in computer forensics. There are commercial training programs such as those offered by the SANS Institute. They provide pretty good training in all parts of the

world. And there are digital forensics product certifications that are also important.

The two main companies whose products you will use are Guidance Software, and Access-Data. Finally, computer forensic investigators need to understand how computers work so companies such as Microsoft and Oracle have certifications that can also be useful."

Kessler considers problem solving, the ability to manipulate symbols and numbers, tenacity, and technical astuteness as traits essential for any good specialist in this field.

"Educational background should be something that supports those traits; ideally - but not necessarily - math, engineering, or computer science but also criminal justice. What people need is the methodical approach to the problem and a well educated person of any stripe can be trained to the level they need, particularly as it relates to conducting investigations," he says, adding that good certifications that are generic and useful include the Certified Computer Examiner (CCE), Certified Forensic Computer Examiner (CFCE), those from SANS, as well as product-specific certs.

"In my career I have hired a lot of people, and there are three general types that I see be successful," says Henseler:

- People with a computer science background who have also worked in a corporate IT department, as they know how companies manage their IT systems. Still, they also need to add the necessary forensics requirements.
- Students who have their masters in forensics investigations but not necessarily in forensic IT. They know how to generate reports but are usually not technical enough. But they need to have a forensic mindset and an avid interest in computers and IT, and to be trained to use the appropriate tools.
- Smart people that have a masters in computer science and who can pick up the forensic tools or can make their own tools. They can become great computer forensic experts, but also good project managers and can help with client communications.

Finally, I wanted to know what are the biggest challenges of the job, and do they consider it to be a hard?

"It is hard job because it is highly technical but you have to also be very precise in your communications," says Hensler.

"There have been big changes over the years. Data starting growing ten years ago and while law enforcement agencies have hired more experts there are not enough experts to go through all the data. The challenge is to enable non-technical people to help investigate so the experts can focus on the most challenging and technical aspects of the investigation," he points out, and to that end he developed Tracks Inspector, a product designed for criminal investigations that enables non-technical investigators to examine evidence themselves.

Kessler thinks that one of the hardest parts about it is the effort needed for staying current. "Many of the criminal cases are also very trying on an emotional level, particularly those involving child sexual exploitation. But, again,

it is very rewarding, too," he says. "I enjoy working with law enforcement because the work is important and they need the help. I don't do criminal defense work but I do engage in civil forensics work."

When asked how he approaches testifying at trials, he says that he talks to judges, juries, and lawyers the way he talks to his students (he's currently on the faculty of the Homeland Security program at Embry-Riddle Aeronautical University, where he is developing a minor in cybersecurity) or his mother: he tries to explain things as simply and accurately as possible, providing no more detail than necessary to illustrate rather than confuse the issues. "In that regard, I view myself as an educator as much as anything else," he shared.

He also says that the prosecution of cyber-criminals is handled pretty well in most cases but could certainly be improved by better preparation of prosecutors and investigators. "We can't control the jury pool and most judges are looking to the attorneys - and their experts - for appropriate explanations."

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security.



People spend
over 700 billion
minutes per month
on Facebook.

Research by Facebook



*The Internet is full of temptations.
Can your users resist them?*

The Internet is one of the most useful resources in the office – but only if you can manage the potential issues:

- » Productivity losses due to employees spending time on sites with little work-related content
- » Security risks: from unsecure sites and from legitimate sites that have been compromised
- » Bandwidth losses from people downloading large files or watching streaming media.

Run the 30-day trial of GFI WebMonitor to find out exactly how your Internet connection and remote machines are being used and what security risks you are exposed to.

Quality web filter

Comprehensive web security

Highly competitive pricing

Thousands of customers

Download your free trial from <http://www.gfi.com/webmon>



GFI WebMonitorTM

Web security, monitoring and Internet access control

UEFI secure boot: Next generation booting or a controversial debate

by Aditya Balapure

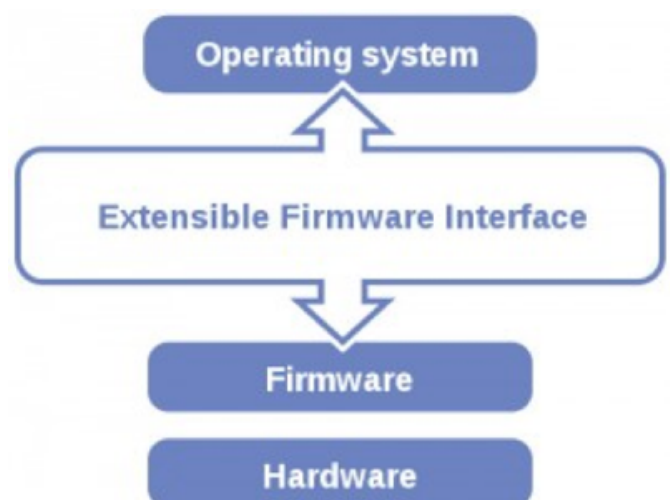


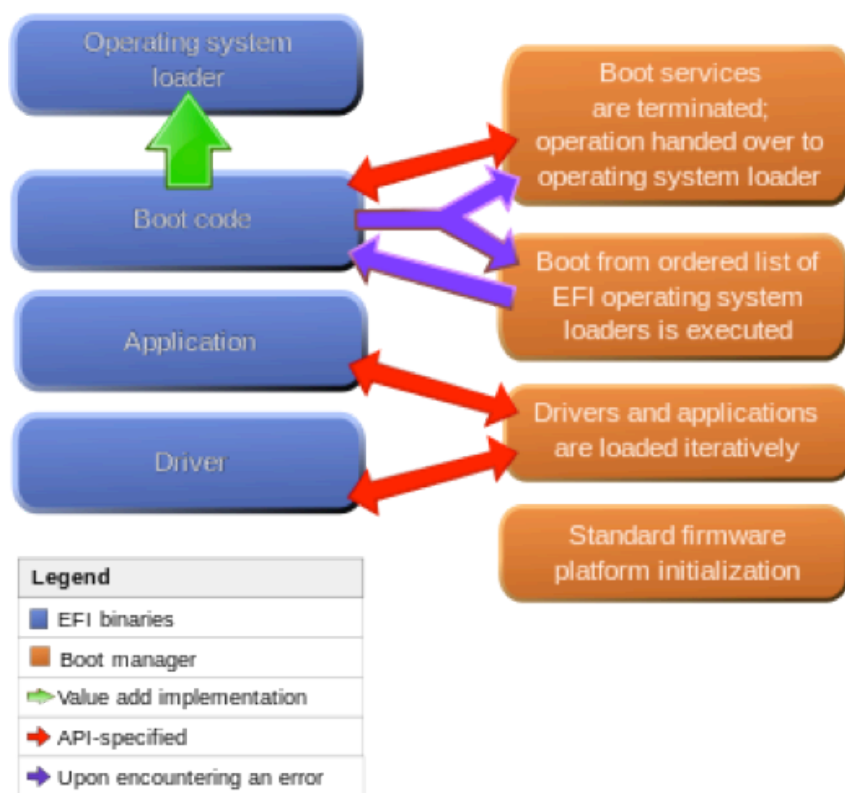
One of the first initiatives for secure booting has been the Unified Extensible Firmware Interface (UEFI) Initiative. UEFI is a superior replacement of the Basic Input Output System (BIOS) and a secure interface between the operating system and the hardware firmware.

The UEFI Initiative was a joint effort by many companies to minimize the risks of BIOS attacks from malware that may compromise the system. It was started by Intel and termed as Extensible Firmware Interface (EFI) for its Itanium-based systems since BIOS lacked the inherent capability to secure vulnerable firmware.

One of the aforementioned BIOS attacks was the Mebromi rootkit, a class of malware that focused on planting itself in the BIOS. Similar to the BIOS, the UEFI is the first program in the booting process and is installed during the manufacturing process of the hardware.

UEFI has the inbuilt capability for reading and understanding disk partitions and different file systems.





UEFI has several advantages, including the ability to boot from large hard disks of around 2TB with a GUID Partition Table, excellent network booting, CPU-independent architecture and drivers. It uses the GUID partition table with globally unique identifiers to address partitions and has the ability to boot from hard disks with capacity of around 9.4 ZB (1024x1024x1024 GB).

Secure boot is a UEFI Protocol to ensure security of the pre-OS environment. The security policy integrated in the UEFI works on the validation of authenticity of components. UEFI has a modular design that gives system architects and hardware designers greater affability in designing firmware for cutting edge computing and for the demand for higher processing capabilities. The sequence of booting remains the same and a computer boots into the UEFI followed by certain actions and ultimately the loading of the operating system.

Furthermore, the UEFI controls the boot and runtime services and various protocols used for communication between services. The UEFI resembles a lightweight operating system that has access to all the computer's hardware and various other functions. The transition from EFI to UEFI continues with Itanium 2 systems followed by System x machines and now we have the new Intel and AMD Series with inherent UEFI capabilities.

How does it work?

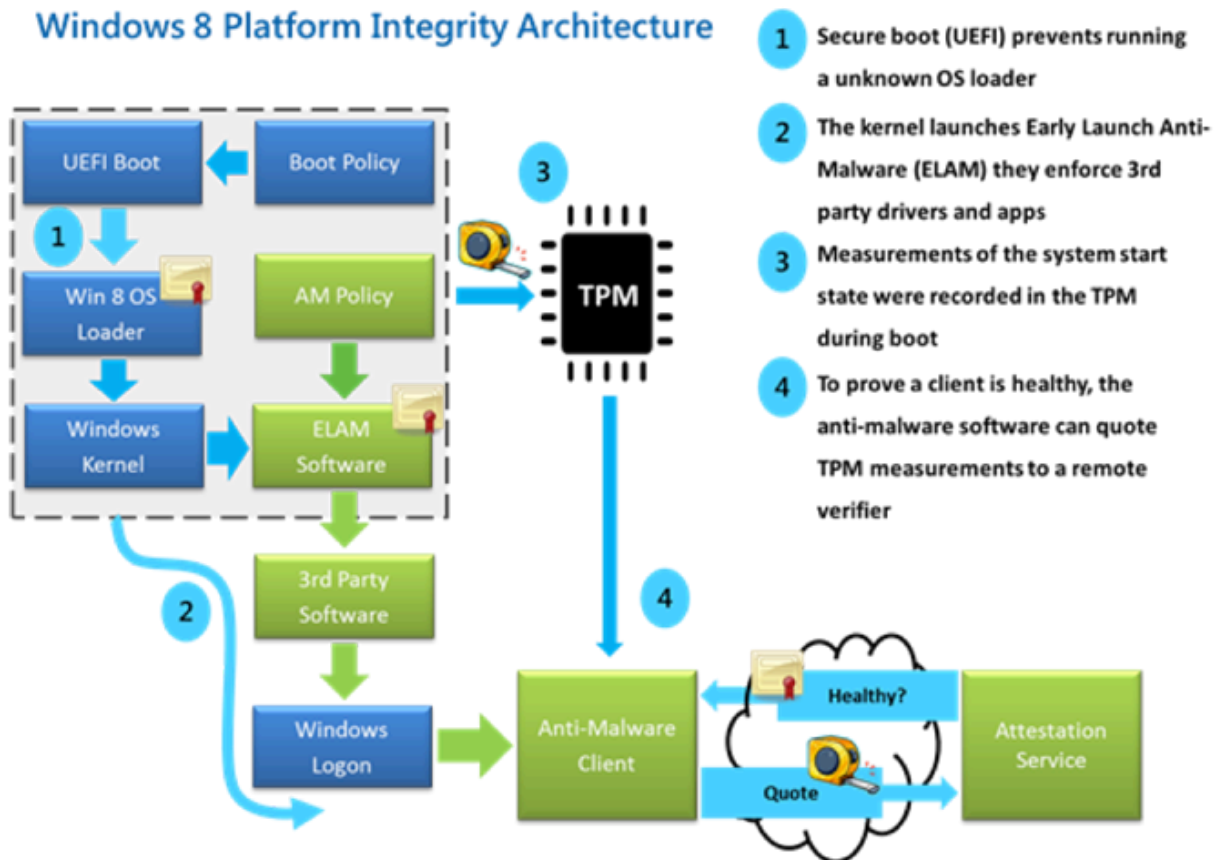
Once we power on a UEFI-capable computer, the code execution starts, and configures the processor and other hardware and gets ready to boot the operating system. As of this date, UEFI has been used with 32/64 bit ARM, AMD and Intel chips and for each of these platforms, there had to be a specific compilation of the boot code for the target platform.

UEFI offers support for older extensions like ACPI, which makes it backward compatible with components that are not dependent on a 16-bit runtime environment. Once a system gets powered on, the firmware checks the signature of the firmware code that exists on hardware components like hard disks, graphic cards and network interface cards. Next Option ROMs work by preparing and configuring the hardware peripherals for handoff with the operating system.

It is during this process that the firmware checks for embedded signatures inside the firmware module against a database of signatures already in the firmware. If a match is found, that particular hardware module is allowed to execute. Hence, it works on a checklist of matching the integrity of signatures from the firmware database and denies further action if a particular component signature is found in the Disallowed list, which means that

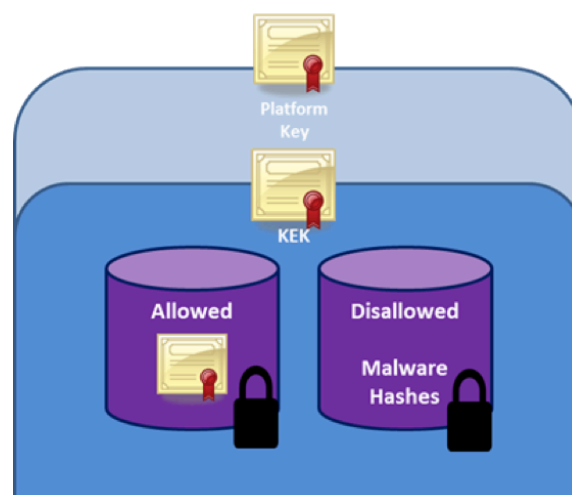
it may be infected with malware. The main database is actually segmented into an Allowed and a Disallowed list. The Allowed list contains the trusted firmware modules while the

Disallowed list contains hashes of malware-infected firmware and their execution is blocked to maintain the integrity and security of the system.



The original equipment manufacturer installs a unique signature and keys during the manufacturing process for the secure booting process. This trust relationship is built on a digital certificate exchange commonly known as Public Key Infrastructure (PKI). PKI is the core infrastructure of the secure boot feature in UEFI. The Public Key Infrastructure is a set of hardware and software policies used to create, manage and distribute digital certificates with the help of a Certificate Authority (CA).

The Secure Boot feature requires the firmware to have UEFI version 2.3.1 or higher. The secure booting feature mainly addresses rootkits and malware that may target system vulnerabilities even before the operating system loads. This feature even protects systems from bootloader attacks and firmware compromises. A cryptographic key exchange takes place at boot time to keep a check whether the operating system trying to boot is a genuine one and not compromised by malware or rootkits.



A while ago there was a dispute between Microsoft and the Free Software Foundation in which the latter accused the former of trying to use the secure boot feature of UEFI to prevent the installation of other operating systems such as different Linux versions by requiring the computers certified with Windows 8 getting shipped with secure boot enabled through a Microsoft private key. Microsoft controls the key signing authority and anyone who wanted to boot an operating system on the hardware certified for Microsoft Windows would have to buy Microsoft's private key at a lucrative price.

The computer hardware would itself have a copy of Microsoft's public key and would use it to verify the integrity of the private key and check whether it is originally from Microsoft. If any modifications are made, the verification would fail and the computer would fail to carry on the boot process any further. Microsoft then denied the fact that this strategy was built to prohibit the installation of other operating systems. It further said that it had the option to either disable the secure boot or allow the Windows 8 boot along with the secure boot feature.

The developers of the open source community were concerned, since most Linux vendors did not have the power to get their certificates in the UEFI system. Red Hat, Ubuntu, and Suse would have no doubt implemented their certificates in the UEFI but the problem lies with communities like Slackware, NetBSD, and others. The main concern was that there are many UEFI motherboard manufacturers and getting the certificates included in each of them would not be an easy task for non-commercial open source communities since it would require a lot of time and money. All the binaries needed to be signed in with certificates from the binaries' vendor, and this was indeed a tough task. And this certificate which signed those binaries had to be imported to the UEFI, which would enable that particular operating system to function securely.

The problem would arise when a hardware vendor would not allow disabling Secure Boot from the setup menu and does not install certificates from other operating systems. In that case, the users who buy the computers with such capability will not be able to make use of

open source Linux operating systems either through dual boot or single boot Linux since the secure boot feature would need the certificate from that particular operating system.

The protests have taken form of Facebook pages like "Stop the Windows 8 Secure Boot Implementation" and campaigns like "Will your computers Secure Boot turn out to be Restrictive Boot" being created.

(www.fsf.org/campaigns/secure-boot-vs-restricted-boot) Hence, until and unless the public key of each open source operating system was available to the hardware vendor, GNU/Linux users would fail to enjoy the combination of secure boot with the inherent security of Linux and if the option to disable the secure boot was not incorporated in that particular hardware by the vendor then life would certainly become very difficult for Linux users.

This secure boot initiative would prohibit tech people from implementing their own custom Linux flavors, and restrict them to using only what the manufacturer of the computer wants them to. The Certifying Authority (CA) would be incorporated by the computer manufacturer and he would ultimately decide whether a particular operating system has to be included or not.

A simple solution to this controversy would be making the user be the CA and giving him or her the authority to decide the choice of operating system with secure boot. But on the other hand, this would open non-technical to the danger of being tricked into using a malicious operating system.

Everything has its pros and cons and that is how technology goes. Luckily, everything is not settled yet and Microsoft is still trying its best without harming the Free Software Foundation and the open source community.

Red Hat, in collaboration with Canonical (the Ubuntu Community) and The Linux Foundation, published a white paper titled UEFI Secure Boot Impact on Linux (tinyurl.com/6es4xcv). For further information regarding Linux and Red Hat, check out the Linux certification courses offered by the InfoSec Institute (www.infosecinstitute.com).

The Red Hat and Canonical team further warned people that the personal computer devices will ship their hardware enabled with Secure Boot, which ultimately would be a problem for the open source distributions.

Although Microsoft clearly denies this fact, the Linux Foundation is full of anger over this initiative. Microsoft is open to the implementation of the option to disable Secure Boot in the UEFI model but, at the same time, it does not strongly support it.

The issue would become even more troublesome if a user wants to dual boot Linux along with Windows. Red Hat along with the Linux Foundation have worked with hardware vendors and Microsoft to develop a UEFI secure boot mechanism that would allow users to run the Linux of their choice. During its research initiative, Red Hat's main aim was to not only provide support to Red Hat/Fedora but also to make users able to run any one they choose.

Red Hat geek Matthew Garrett, put forward a customized solution in which Microsoft would provide keys for all Windows OS, and Red Hat would similarly provide keys for Red Hat and Fedora. Ubuntu and others could participate by paying a nominal price of 99\$. This would allow them to register their own keys for distribution to firmware vendors.

We have covered the advantages of having the Secure Boot feature of UEFI, but there are cons to be considered as well. Having the Secure Boot feature would require all the components of the system to be signed, which includes not only the bootloader, but any hardware drivers as well. If the component vendors wished to sign their own drivers, they would need to ensure that their key is installed on all hardware they wish to support. For laptops, a single point solution would be to make all the drivers be signed with the OEM's keys.

At the same time, this approach would be problematic for the new hardware vendors and would prevent them from entering the new market until they distributed their keys to

major OEMs. An alternative approach could be to have the drivers signed by a key included in the majority of the platforms. This would help hardware vendors from having per-platform issues. Also, if secure boot is disabled to boot an alternate OS, then this process would be limited to those who are technologically-savvy, i.e. not for the masses.

Another disadvantage to the signing process is that if the signing key is disclosed and gets in the wrong hands, it may be used to boot a malicious operating system even with Secure Boot restrictions. To avoid this, the signing key would have to be blacklisted, which would prevent the operating system from booting. If the same happens with hardware vendors then the drivers would not validate and would cease the system process.

We come to a point that the UEFI Secure Boot technology is a crucial part of a Linux setup and increases the protection at the root level to fight against the use of malicious software. The only limitation is that it should not hinder user freedom by limiting its use of different operating systems.

The sad part is that the current version of Secure Boot model deters easy installation of Linux and inhibits users to play with the whole system. After a long research initiative, the open source community recommended that the Secure Boot implementation is designed around the hardware vendor who would have full control over security restrictions.

It is also recommended that the original equipment manufacturer should agree with allowing the secure boot option to be easily disabled and enabled as per the user's choice. (This means that secure boot may be disabled through the OS and you may have the option to enable it through the firmware interface something like BIOS has.)

This would help the open source community and also help the cause of the Secure Boot initiative.

Aditya Balapure is an information security researcher, consultant, author with expertise in the field of web application penetration testing and enterprise server security.



How to detect malicious network behavior

by Stephen Newman

When dealing with the stealthy nature of today's advanced threats, the major indicators of attacks and compromises appear in the enterprise's network communications.

Detecting malicious network behavior is a growing challenge. Security devices and software are not evolving nearly as fast as the attacks they are up against. As a result, many defense-in-depth solutions like intrusion detection systems and antivirus fail to catch attacks.

Further complicating the matter is the fact that attackers have more resources at their disposal than most IT security teams, and one objective on which they can focus all their time and money. For the IT security team, stopping attackers from achieving their objectives is just one item in a long list.

Given these challenges, IT security teams need to adopt a new approach to detecting malicious network behavior; one that leverages the very infrastructure used by attackers. It is possible – if you understand the kill chain and what to look for.

Understanding the kill chain

The kill chain is a systematic process attackers use to carry out an attack campaign. It consists of the following phases:

Reconnaissance – The target is profiled and information about the target is collected, including the organization's structure, basic security controls, etc.

Weaponization – Malicious code is prepared to exploit a vulnerability on a target device along with the creation of malware that will be dropped onto the exploited device

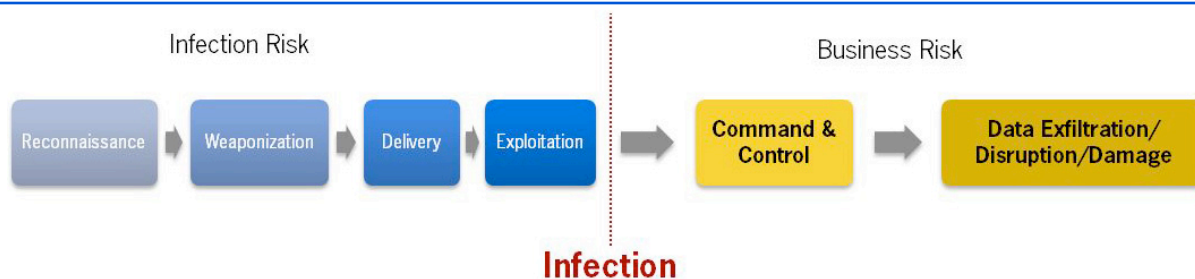
Delivery – A campaign is created to entice the targeted user to perform action such as clicking on a link or visiting a web page that exploits a vulnerability on the device.

Exploitation – The exploit code is executed on the target device, enabling the attacker to

download the initial “dropper” malware and providing the attacker control. This can be a multi-stage process wherein the dropper obtains control of the device and then downloads additional malicious code designed to perform data exfiltration or damage to the target network.

Command-and-control – The compromised (infected) device contacts its control network to receive further instructions or retrieve additional malicious code.

Exfiltration – Data is removed from the network while attempting to avoid detection.



After Infection Takes Place, the Game Changes

Attackers use the network to carry out the exploitation, command-and-control, and data exfiltration phases of the kill chain and, in doing so, leave a trail of breadcrumbs that can lead right to the infected system.

Performing network-based threat discovery

Network-based threat discovery refers to utilizing the information you can glean from the network regarding attackers’ actions as they proceed through the kill chain. You can uncover hidden infections through profiling a device’s network-communication and asking five key questions: how / when / what / where and who. Evidence attributed to any one of these questions is not enough to pinpoint an infection. However, if two or more of the questions are answered and corroborated, together they build a case to discover an infection that was previously hidden.

How / when: Behavior analysis

Unlike broad network behavioral analysis techniques which establish a baseline for the entire network’s communications, if you profile the behavior of each individual device you can differentiate between human based activity and automated software based activity (like that of malware communicating to the attacker). Listening to each device’s Internet-bound communication attempts enables the discovery of automated communications such as temporal based anomalies (when), domain

fluxing activity (how), or non-benign peer-to-peer attempts (how).

What: Content analysis

During the exploitation and command & control phases, the content of the communications can also serve as key evidence of an infection. For exploitations and subsequent malware drops that occur while a device is within the corporate network, signature-less identification and real-time analysis of these files being transferred to or from a device can indicate potential infections and provide clues as to “what” infection is present.

Capturing a copy of these files and executing them in a virtual environment to identify their behavior provides the fastest mechanism to discover new malicious code. Other content analysis such as request header analysis can reveal the type of malware family based on the communication language used between an infected device and the attacker.

Where / who: Threat intelligence and attribution

Profiling where any device is communicating on the Internet can reveal command and control activity. While blacklists and cyber intelligence information sharing is valuable, it also can generate immense noise and false positive alerts as command and control destinations change frequently or utilize hacked legitimate sites. As a device communicates with

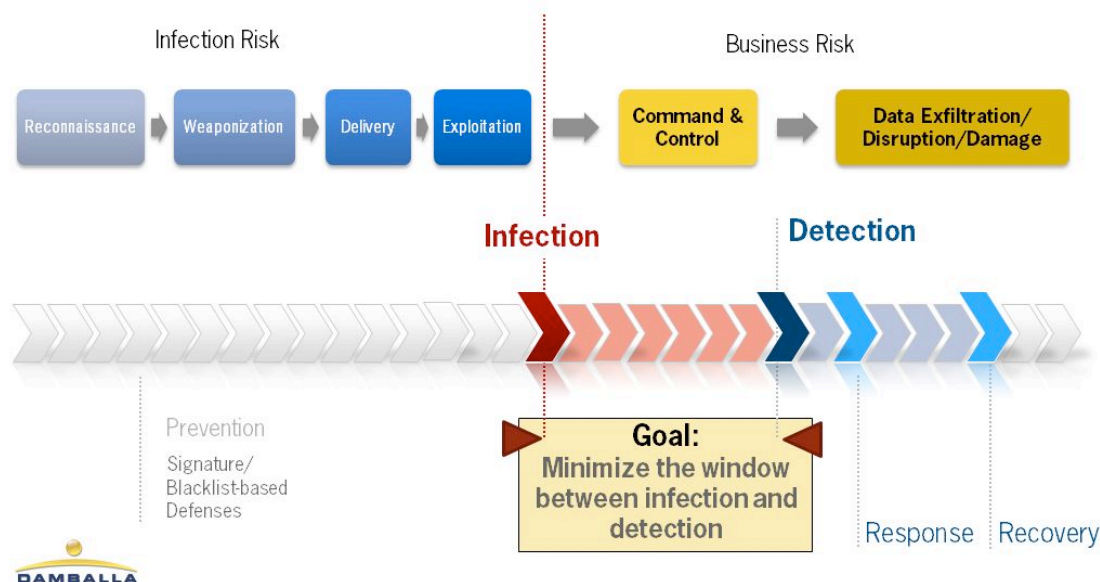
shady Internet destinations it is important to consider the relationships of the destinations to malware families and ultimately to the attacker as threat actors are not limited to only one type of malware or one malicious destination. Comparing the “where” and “who” a device is communicating to with the “how” and “when” the communication persists over time provides the ability to pinpoint a hidden infection.

How to utilize network-based evidence

Network-based evidence can be used both for forensics purposes and to shorten the time between a compromise (infection) and detection. The collection of this evidence into

SIEMs and log aggregators can provide invaluable forensic evidence to go back to and examine after the discovery of an infection. However, these products are reactive in nature for the discovery of a hidden infection. In order to achieve the goal of shortening the time between a compromise and detection, IT security teams need to complement their efforts with another solution that is designed to identify advanced threats as they are happening.

Today’s complex attacks are successful in large part because they are dynamic. Attackers are constantly changing their targets, algorithms, domains and everything else they use in the kill chain.



Attacks, therefore, are more efficient, obscure and resilient. To play this game effectively, you must also adapt your organization’s approach to them. Reliance on solutions that only alert on evidence from a single point in time are not sufficient. Enterprises are now looking to solutions that can ask the questions how, when, what, where, and who of network traffic in real-time and assess the answers to corroborate evidence and discover advanced threat infections.

In order to close the gap, consider partnering with a provider that has a full deep packet inspection engine and a framework that allows new detection techniques to be added.

Look for one who can deliver evidence of an infection to you in a useful manner and enable you to be agile in responding to discovery of new infections.

Conclusion

Attacks against networks have evolved beyond the capabilities of our traditional defense technologies. It is time IT security teams change the way they protect the network. With an understanding of the kill chain and the trail of breadcrumbs generated during an attack, IT can level the playing field once more. And with a partner to automatically ask the relevant questions of your network traffic, organizations can achieve the agility that will help them tip the playing field in their favor.



Microsoft Citadel takedown ultimately counterproductive



The disruption of nearly 1500 Citadel botnets believed to be responsible for over half a billion US dollars in financial fraud and affecting more than five million people in 90 countries has been welcomed by most security experts, but not all.

According to Swiss security expert Roman Hüssy who runs the Zeus, SpyEye and Palevo Trackers, the action effected by Microsoft in conjunction with the FBI and several industry partners has inflicted considerable damage to his and other researchers' efforts.

"As a security researcher I spend a lot of time in researching botnets in my spare time, and abuse.ch is running such a sinkhole as well. The goal is simple: sinkhole malicious botnet domains (not only limited to any specific Trojan / malware family) and report them to Shadowserver," he explains.

"Shadowserver, a non-profit organisation like abuse.ch, then informs the associated network owners about the infections reported by my sinkhole, in addition to infections reported by their own sinkholes and sinkholes run by other operators. In fact, every Computer Emergency Response Team, Internet Service Provider and network owner can get a feed from Shadowserver for their country / network for free."

But with the recent takedown, a number of domains he sinkholed started pointing to a server in Microsoft's network range. Additional research revealed that over 300 domain names that where sinkholed (and appropriately tagged) by him were also "seized" by Microsoft.

New Android Trojan is complex as Windows malware



Mobile (and especially Android) malware is on the rise and according to researchers from Kaspersky Lab, its complexity is also increasing. Case in point: Backdoor.AndroidOS.Obad.a.

This newly discovered Trojan has obviously been constructed by someone who knows quite a bit about the Android platform, as the creator has taken advantage of multiple known and previously unknown errors and vulnerabilities in the OS to make the analysis of the file difficult.

An error in the software program used by analysts to convert APK files into the (for the analysis) more convenient JAR format has been used to prevent such a transformation, complicating thusly the statistical analysis of the Trojan.

Two bugs in the Android operating system itself have been used to modify a file that makes dynamic analysis of the malware harder, and to extended Device Administrator privileges to the app, but without making it obvious (i.e. adding it to the list of applications which have such privileges.).

This, and the fact that the Trojan does not have an interface, makes it impossible to delete it once the device is compromised. The creators have also done a good job in encrypting and obfuscating most of the code - strings, names of classes and methods.

The Trojan is able to do a number of things: blocking the device's screen for up to 10 seconds; harvesting information such as the name of operator, phone number, IMEI, phone user's account balance, whether Device Administrator privileges have been obtained and send it to a remote C&C server; downloading additional malware; sending messages to premium-rate numbers; sending the download malware to other nearby devices via Bluetooth, and so on.

Researchers find self-propagating Zeus variant



The Zeus / Zbot Trojan has been around since 2007, and it and its variants continued to perform MitM attacks, log keystrokes and grab information entered in online forms.

It is usually spread via exploit kits (drive-by-downloads), phishing schemes, and social media, but Trend Micro researchers have

recently spotted a variant that employs another propagation vector: removable drives.

In this particular instance, the malware variant is initially delivered via a malicious PDF file disguised as a sales invoice document.

Potential victims that attempt to open the file with Adobe Reader are faced with a notice that says that it can't be opened because "use of extended features is no longer available."

But in the background, the malware has already been silently dropped onto the system and run.

It first contacts its C&C center to download an updated copy of itself (if there is one available), but immediately after it checks whether removable drives are connected with the computer, and if there are, it drops a copy of itself in a hidden folder, then creates a shortcut to it.

Fake Mt. Gox pages aim to infect Bitcoin users



Mt. Gox is the the largest Bitcoin exchange in the world, and as such it and its users are being repeatedly targeted by attackers.

Two months ago, it battled a massive DDoS attack that was likely aimed at destabilizing the virtual currency and allow the criminals to profit from the swings.

Now, according to Symantec researchers, the criminals have turned to spoofing Mt. Gox' site and tricking its customers into downloading malware - the Ponik downloader Trojan, which is also able to steal passwords.

This fake pages were set up on domains that resembled Mt. Gox' legitimate one (mtgox.com), such as mtgox.org, mtgox.co.uk, mtgox.net, and others. Also, the criminals

have done a good job promoting the phishing site via ads ("New Century Gold: BITCOIN Protect your money - Buy Bitcoin") served by several major online advertising services.

The fake page is a pretty good spoof of the legitimate one, but there are details that reveal its real nature. For example, the phishing page does not use the SSL security protocol (i.e. there is no https in the URL).

"Mt.Gox has started to intensify the verification process of its members, allowing deposits or withdrawals only from verified accounts. They appear to be doing as much as possible to comply with anti-money laundry laws in order avoid the same fate as Liberty Reserve, which was shut down by federal prosecutors in May," Symantec researchers pointed out, and advised users to change their passwords and verify their accounts.

Users who have fallen for this particular phishing scam would also do well to check their computers for this and other malware.

Cyberespionage campaign targeting government-affiliated organizations



NetFile-801.exe
版权所有 (C) 2004

Kaspersky Lab experts published a new research report about NetTraveler, which is a family of malicious programs used by APT actors to successfully compromise more than 350 high-profile victims in 40 countries.

The NetTraveler group has infected victims across multiple establishments in both the public and private sector including government institutions, embassies, the oil and gas industry, research centers, military contractors and activists.

Attackers infected victims by sending clever spear-phishing emails with malicious Microsoft Office attachments that are rigged with two highly exploited vulnerabilities (CVE-2012-0158 and CVE-2010-3333). Even though Microsoft already issued patches for

these vulnerabilities they're still widely used for exploitation in targeted attacks and have proven to be effective.

During Kaspersky Lab's analysis, its team of experts obtained infection logs from several of NetTraveler's command and control servers (C&C). C&C servers are used to install additional malware on infected machines and exfiltrate stolen data. Kaspersky Lab's experts calculated the amount of stolen data stored on NetTraveler's C&C servers to be more than 22 gigabytes.

Exfiltrated data from infected machines typically included file system listings, keylogs, and various types of files including PDFs, excel sheets, word documents and files.

In addition, the NetTraveler toolkit was able to install additional info-stealing malware as a backdoor, and it could be customized to steal other types of sensitive information such as configuration details for an application or computer-aided design files.

New Mac spyware signed with legitimate Apple Developer ID



A new piece of malware designed to spy on Mac users has been unearthed by security researcher and hacker Jacob Appelbaum at the Oslo Freedom Conference held in May in Norway.

The malware was discovered on an African human rights activist's Mac who participated in a workshop dedicated to teaching activists how to secure their devices against government and any other kind of snooping.

"The Angolan activist was pwned via a spear phishing attack – I have the original emails, the original payload and an updated payload," Applebaum explained in a tweet.

The worst thing is that the malware wasn't, at the time, detected as such by any security software, and neither were the URLs serving it. In fact, the backdoor was signed with a legitimate Apple Developer ID associated with a developer by the name of Rajinder Kumar, and thus was able to bypass Apple's Gatekeeper.

The malware starts working every time the computer is restarted, and it takes screenshots in regular intervals and uploads them to two C&C servers - one of which is currently unavailable, and the other impossible to access without permission. Since the discovery of the malware, Apple has revoked the aforementioned developer's ID, and another researcher has discovered another sample in the wild.

The good news is that the malware can easily be removed from the infected computer by deleting macs.app from the applications folder and log-in queue.

According to the folks at F-Secure, the malware is connected with a large cyber espionage campaign originating from India.

Can mobile malware be activated via sensors?



Can mobile malware be activated via sensors available on current mobile devices, and receive commands through out-of-band communication methods?

If you ask a group of researchers from the University of Alabama at Birmingham and the Polytechnic Institute of NYU, the answer is yes.

To prove their theory, they have created and tested proof-of-concept Android apps that received command and control trigger messages from a distance of 55 feet indoors and 45 feet outdoors, sent by using only low-

end PC speakers with minimal amplification and low-volume.

In theory, such a signal can be incorporated into TV or radio programs, background music services, Internet TV program and even musical greeting cards, and the signal is received even if the device is located in a user's pocket.

When it comes to light signals, they discovered that they work best when it's dark out, or if the device is in a poorly lit environment, and that magnetic signals have the shortest range because they are quickly dispersed as they travel through the air. Nevertheless, the researchers say that magnetic signal transmitters can easily be incorporated into places where users are bound to be come in range (tight passages such as doorways or door frames, and very crowded areas).

Scanner identifies malware strains, could be future of AV



When it comes to spotting malware, signature-based detection, heuristics and cloud-based recognition and information sharing used by many antivirus solutions today work well up a certain point, but the polymorphic malware still gives them a run for their money.

At the annual AusCert conference in Australia, security researcher Silvio Cesare has presented the result of his research and work that just might be the solution to this problem. He had noticed that malware code consists of small "structures" that remain the same even after moderate changes to its code.

"Using structures, you can detect approximate matches of malware, and it's possible to pick an entire family of malware pretty easily with just one structure," he shared with CSO Australia.

He created Simseer, a free online service that performs automated analysis on submitted malware samples and tells and shows you just how similar they are to other submitted specimens. It scores the similarity between malware (any kind of software, really), and it charts the results and visualizes program relationships as an evolutionary tree.

If a sample has less than 98 percent similarity with an existing malware strain, the sample gets catalogued as a completely new strain.

According to the website, Simseer detects malware's control flow, which changes much less than string signatures or similar features, and polymorphic and metamorphic malware variant usually share the same control flow.

It runs on an Amazon EC2 cluster with a dozen or so virtual servers, and is "fed" by Cesare every night with gigabytes of malware code downloaded from other free sources such as VirusShare. So far, Simseer has identified more than 50,000 strains of malware, and the number keeps growing.

Cyber espionage campaign uses professionally-made malware



Trend Micro researchers have discovered a new, massive cyber espionage campaign that has been hitting government ministries, technology companies, academic research institutions, nongovernmental organizations and media outlets.

Dubbed "Safe," the campaign has first been spotted in October 2012 and has so far resulted in nearly 12,000 unique IP addresses spread over more than 100 countries to be connected to two sets of C&C infrastructures, but the actual number of target seems to be smaller as some of these IP addresses were concentrated within specific network blocks so are probably used by the same organization.

One of the C&C servers was set up in such a way that the contents of the directories were

viewable to anyone who accessed them. As a result, not only were we able to determine who the campaign's victims were, but we were also able to download backup archives that contained the PHP source code the attackers used for the C&C server and the C code they used to generate the malware used in attacks.

The attacks start almost predictably via Tibetan- and Mongolian-themed spear-phishing emails containing a malicious MS Word file specifically designed to exploit a vulnerability (CVE-2012-0158) in older versions of the software.

The decoy document would open, and in the background malicious files would be dropped onto the system in preparation for the second stage of the attack: the downloading and running of additional malware and tools such as off-the-shelf programs that are able to extract saved passwords from Internet Explorer and Mozilla Firefox as well as any stored RDP credentials.

SECURITY AWARENESS FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.

- Create your own program by choosing from 30 different training modules.

- Meets requirements of the Data Protection Act and PCI DSS.

- Training is mapped against the 20 Critical Control framework.

- For more information visit us at www.securingthehuman.eu



www.securingthehuman.eu

What startups can learn from enterprise level data security tactics

by Dr. Hyeyeon Ahn



Even the most innovative or forward-thinking startups rarely have the resources necessary to pay for enterprise-level data security options, yet they certainly share a similar need to protect sensitive information.

One mistaken email or stolen iPhone containing potentially priceless intellectual property could spell disaster for any such startup. There is hope though.

Much can be learned from the tactics of larger enterprises, and when done right, startups can use these cues to implement comprehensive advanced security practices for a fraction of the cost - or even for free.

To develop a strategy around the ever growing need for data security, startups and SMBs must examine their unique security challenges before exploring the applicable enterprise-level security tactics and best practices which they will look to mimic.

With that understanding in hand, they can build their data security measures in a way that works on their smaller scale.

The security challenges faced by startups

The first challenge any startup faces relates to their available resources, both on the financial and personnel fronts. Startups are by nature rich in ambition, but rarely find themselves rich in resources. Startups do not have the luxury of paying for some of the much-needed capabilities featured in the costly tools and programs enterprises use.

Additionally, at a fledgling business, the CEO often wears many hats, serving as dynamic leader, accountant and in-house IT team.

In the role of the de facto IT department, the CEO's first major challenge is to establish a way to store and share information while enabling collaboration across a fragmented and mobile personnel group. While enterprises can employ costly network infrastructure, this isn't always an option for startups due to sheer cost. That leaves many emerging businesses searching for other ways to share and save information.

With more recent technological developments, many startups are finding tools that are similar to those enterprises use, but at a smaller, more affordable scale. It should come as no surprise that they routinely turn to consumer-driven cloud services like Dropbox, which has more than 100 million users, or other popular services like SugarSync, Box, and YouSendIt to enable collaboration.

Dropbox in particular has catered to startups and SMBs with features that make it easier for teams to collaborate and managers to keep track of account usage. Undoubtedly, such

cloud services make collaboration and file sharing more effective, increasing productivity within the overall workflow. Email also remains a popular way to share files, though it lacks the real-time collaboration and version control that cloud services offer.

While collaboration is vital for successful startups, there are inherent risks associated with sharing sensitive information via email or the cloud. At any given time, proprietary company and client information, unpatented intellectual property, or financial records being shared via email or in the cloud are susceptible to loss or even theft.

Collaboration breeds security threats posed by third-party providers, cloud technology itself, and, of course, user behavior, with data breaches often happening because of a simple human error. As a recent example, more than 126 billion files uploaded to a consumer cloud service were compromised when users inadvertently changed their privacy settings.

Data leaks can come from multiple sources including malicious email or cloud hacks, device theft, and simple human errors.

User behavior becomes a compounded concern with many startups saving on resources by implementing bring-your-own-device (BYOD) policies, which exponentially increases the potential points of data vulnerability. The challenge with employee-owned devices is that it is difficult to enforce a policy that requires everyone to have the same security. With the combination of cloud technology vulnerability, the potential for user error during collaboration, and an expansive array of unsecured standalone hardware devices, it is difficult to control information, leaving companies at risk for potentially devastating data leaks.

Data leaks can come from multiple sources including malicious email or cloud hacks, device theft, and simple human errors. According to the Online Trust Alliance, more than one hundred thousand email accounts are hacked each day, and recent Forrester survey data

indicates that company insiders and business partners account for 43 percent of security breaches. From intentionally or unwittingly changing settings, to simply sending a file to the wrong person, it's often human error that poses the biggest threat to data within a company. Accommodating the human factor is often the most daunting challenge that a startup will face as it explores its security needs.

Key tactics for enterprise security

While budget, staffing and in-house capabilities dramatically separate enterprises from startups, there is significant overlap in the types of risks they face. Similar data – proprietary information, personnel records, unpatented intellectual information, tax information, and legal documents – all need to be protected within an enterprise and startup venture.

Unlike smaller companies that may be using free or low-cost cloud storage services as their “network,” enterprises must also take precautions to protect the network itself. Enterprises have to maintain their own network, IT infrastructure and resources like dedicated groupware, file servers, etc.

Because of the more complex network and infrastructure, several kinds of security solutions will be needed. This usually starts with firewalls and anti-malware, and can expand to more comprehensive data-centric security solutions including digital rights management (DRM) technology.

Traditional IT security was built to protect and secure devices that are managed by the internal infrastructure. But with the rise of smart devices including smartphones and tablets, enterprise IT departments have had to grapple with both managed and unmanaged devices.

The trend at the enterprise level is now moving toward using unmanaged devices and even encouraging BYOD programs that re-

quire policies to help govern device usage and maintain a secure environment.

As workforces become more mobile, using a mix of organization-managed and personal devices, information security is being challenged to facilitate that mobility while simultaneously protecting information by detecting, controlling, and preventing threats.

As a result of having more mobile devices and more employees using cloud services that are not controlled within the internal infrastructure, IT departments are simply unable to control data as they once were.

Encryption technology takes prominence in this evolved enterprise environment. The benefit of encryption is that it can be applied across the employee workflow from the dedicated IT infrastructure, through public cloud services to the employee-owned devices. By directly protecting the content itself, rather than just the network, encryption technology can be the most powerful and easily implemented security solution available to enterprise and startups alike.

DRM encryption offers persistent protection so files do not need to be decrypted before accessing or editing.

How startups can adapt these enterprise best practices

For startups, the BYOD model offers an affordable and flexible platform for their growth, and they can learn from enterprise security strategies by building their own comprehensive BYOD policies. These policies need to address the unique security concerns of startups, which include securing multiple types of devices and protecting data saved to public cloud services. Key considerations for such a policy should include:

- Creating and enforcing a mobile policy either on personal devices or separating business and personal environments
- Maintaining a baseline of allowed supported devices
- Offering the option for enterprise-owned devices or a mobile device for work purposes.

The next transferable lesson is to create a more data-centric-security strategy rather than perimeter-based protocols of the enterprise. This approach needs to start with a DRM tool that combines advanced encryption techniques to secure data. This allows startups to encrypt files themselves before emailing or sharing via public cloud providers.

Unlike simple encryption which has limitations, DRM encryption offers persistent protection so files do not need to be decrypted before accessing or editing. Because the files are protected before being introduced to any external threats, they are secure no matter how many devices an employee uses to access the file.

DRM functionality varies between offerings, so startups should look for a few key capabilities in their selected tool, including:

- Ease of use and seamless integration with the business workflow, with encryption as simple as a right-click option or a drag-and-drop
- Advanced data encryption techniques that rely on AES-256, an encryption algorithm trusted by the United States government to protect classified information
- An easy-to-use permissions interface to control who can access files, and what they can do with them – including read-only, print, or editing capabilities – and the ability to change those permissions at any time, even after a file has been shared
- A file audit log that provides visibility to who, what, when and where files are being used
- A mobile platform that ensures the DRM and encryption permissions can be accessible

from anywhere – this is often available through a companion mobile app.

By implementing some of these enterprise practices, startups can enjoy the benefits of technologies like public cloud providers, mobile devices and encryption services to ensure their business is protected. In particular, using DRM features results in better file management that extends beyond the boundary of desktops to mobile devices. DRM solutions provide persistent and reliable protection that includes file encryption, permission control, and audit trail technologies.

By protecting the files themselves, startups can safeguard and prevent unauthorized use of files – no matter where they are saved or how they are shared.

Dr. Hyeyeon Ahn is the vice president and CTO at Fasoo.com (www.fasoo.com), an enterprise digital rights management company.

FRESH SECURITY NEWS

www.twitter.com/helpnetsecurity

twitter



To hack back or not to hack back?

by Kai Roer

If you think of cyberspace as a new resource for you and your organization, it makes sense to protect your part of it as best you can. But is it a good idea?

Many centuries ago, explorers came to the vast land of North America. Shipload upon shipload of dreamers, explorers, businessmen and farmers entered the harbors and spread out throughout the country. They all dreamed of a better life - however they defined it. As population in the West gradually grew, the need for stability and peace did too. In the very beginning, a gun and the principle of “an eye for an eye” allowed the survival of the best gun-hand, often at the detriment of many a young farmer with lesser gun-slinging skills. This self-regulation has been referred to as the Code of the West.

But after a time it became evident that shoot-outs in the streets were counterproductive to stability, peace and predictability. The principle of self-protection had to give way to another principle. Thus the law came to the West, and replaced the Code. Individuals gave up (or were forced to give up) their right to pursue justice individually, and handed the task of prosecuting, judging and possibly executing criminals over to the government.

A new resource

If you think of cyberspace as a new resource for you and your organization, it makes sense to protect your part of it as best you can. You build fences to keep your cattle in, and the horse thieves out. You train your cowboys to ride and shoot well, and to recognize newcomers for what they are. And you accept the fact that your government is the one that will pursue and prosecute the thief that stole one or more of your horses.

The challenge arises when you (possibly rightfully so) perceive that your government is not able to deal with the horse thief. In the Wild West, you would have your cowboys string him up and hang him.

In cyberspace, you demand to be allowed to “hack back”. You want your government to delegate the legal persecution, judging and execution to you, because (you claim) you know the situation better.

You may find yourself saying something along the lines of: "Our cyberjockeys are highly skilled, quick to shoot and fully capable of taking down any trespassing hacker. I must have the right to defend myself, and attack is the best defense. Because, my dear government, if I do nothing, it will only be a matter of time before they enter my premises and run me over."

From your narrow and personal perspective, this kind of reasoning may make sense at first glance. This is the same kind of reasoning that feeds blood feuds through the principle of "an eye for an eye" — "if you kill someone in my family, I will kill someone in yours. Innocent or not, I will shoot." And so it goes until both families are no more.

Without an overarching governing body, instability, violence and uncertainty become the rule of thumb. It's obvious that larger groups of humans who need to interact, interconnect and work together need a governing body to sort out disputes and acts of criminality. A legal system is here to help each one of us, but we have to accept that it may not be perfect, and that it may take some time to adjust it to the cyber domain.

Gut response or intellectual reflection?

A gut response to direct threat is retaliation (or you may choose to run and hide). Consider that we are all part of a global community these days. It is not only you and that horse thief anymore. It is you, your employees, your country, your country's trade partners, and so forth. In cyberspace, you cannot act like a rogue player who does whatever comes to his or her mind. Your playground is no longer your own backyard where you can argue "self defense" and get away with it.

The implications of hacking back are much larger than you and your organization. What you think of as a simple retaliation operation may quickly evolve into a geopolitical situation with multilateral impact.

It is one thing to shoot a horse thief, and it is a very different thing to accidentally trigger a nation-state's war machine. I urge you to take

a moment to think things through. Use your intellectual capacity to reflect on what is better - a closed-down world where everyone shoots at each other, or a world where we all abide to the same laws made out to build global stability, peace and predictability?

Patience, my friend

Yes, the current laws and legal systems are a major challenge to cybersecurity. History has shown us that allowing every man his own justice system simple does not scale well. We do not need a granulated "hack back" retaliation regime.

We must focus our efforts on making an international cyber governing body that will decide the laws and that will have the authority to pursue and make justice across national and regional borders. Personally, I would not mind hearing a prosecutor say: "The World versus Hector Hacker."

We need a new system, and that system must be larger than each individual, organization and nation-state. Obviously, the creation and implementation of such a multilateral governing body will take time and effort. While we are waiting, we can help by pushing our governments in the right direction. Open dialogue, building trust and sharing information are important building blocks. Respecting differences, and seeking to learn how to overcome them is vital.

Private organizations may help by setting up and funding think-tanks, inviting both public and educational sectors to discuss alternative courses of action. Nation-states can help by using existing governing bodies like WHO, UN and Interpol to create a new, global cybersecurity unit, and enter into agreements that enable it to govern the sector on a global perspective.

Every single one of us can look beyond mere self-interest, and look for common ground where workable, realistic solutions can grow and operate. And have the patience to allow for this process to evolve and grow, just like it happened when the Code of the West was replaced by law.

ELEVENTH ANNUAL
HITB SECURITY
CONFERENCE
IN ASIA

REGISTER ONLINE

<http://conference.hitb.org/hitbsecconf2013kul/>

HITBSECCONF2013 KUALALUMPUR

October 14th - 17th 2013 @ InterContinental Kuala Lumpur

8 NEW TRAINING COURSES (14th - 15th October)

- Extreme Web Hacking
- Windows Kernel Internals
- Blackbelt Penetration Testing
- The Art of Exploiting Injection Flaws
- The Android Exploit Lab
- Advanced iOS Exploitation
- Introduction to iOS Exploitation
- Building Secure Web & Mobile Applications

CONFERENCE KEYNOTE SPEAKERS (16th - 17th October)



ANDY ELLIS (Chief Security Officer, Akamai)



JOE SULLIVAN (Chief Security Officer, Facebook)

Report: Infosecurity Europe 2013



With 13,200 visitors, Infosecurity Europe is an important event in the European calendar for IT security. Not only did it bring together the entire security community, with many attending for at least two days, but it was where companies chose to reveal innovations and launch products.

The 2013 show attracted a 6% increase in visitors compared to last year, as well as a record number of global representatives, with over half of the vendors coming from overseas and visitors from over 110 different countries – coming from as far as South Korea, Australia, Singapore, Turkey and Hong Kong. The show

also provided a showcasing platform for over 50 new exhibitors, including a larger French pavilion and brand new Russian and German pavilions, which housed a range of new IT security vendors.

The show saw a significant increase in people revisiting over the three days, which highlights the thought-provoking education program – the show included 17 keynote sessions, all of which are specially selected by Information Security Hall of Fame members, guaranteeing delegates innovative topics.





Visitors to the show also benefited from 31 sessions in the Business Strategy Theatre, 31 sessions in the Technical Theatre, 14 in the Information Security Exchange, 17 IT security workshops as well as 24 seminars in the Technology Showcase Theatre.

Some of the key highlights included: a presentation from the UK's Minister for Political and Constitutional Reform with responsibility for cyber security – Chloe Smith – who delivered a keynote speech covering the government's determination to keep the UK safe from cyber-crime; and Symantec ran a hacking challenge

where IT security professionals were asked to observe other experts testing their skills and knowledge in a 'capture the flag' style cyber attack simulation, where players competed against each other to solve IT security problems.

“Visitors were far more engaged - refreshing to see the curiosity and interest – we saw lots of qualified leads, with masses of activities around the stand drawing on the customers.” said Amer Deeba, CMO, Qualys.



Then there are those attacks that use DNS as a vector for business exploitation; these include attacks such as botnets, domain phishing, APTs or tunneling frauds.

Here is a summary of the most important threat vectors among them:

Cache poisoning: In this attack, the perpetrator sends spoofed DNS responses to a DNS resolver, which are then stored in the DNS cache for the lifetime (time to live [TTL]) set. A user whose computer has referenced the poisoned DNS server would then be tricked into accepting content coming from a non-authentic server and would unknowingly download malicious content.

DNS protocol attacks: In this attack, the perpetrator sends malformed DNS queries or responses to the target DNS server and allows the exploitation of protocol implementation bugs in the server's software. Examples include malformed packets, code insertion, buffer overflows, memory corruption, NULL pointer dereference or the exploitation of specific vulnerabilities. The result of these attacks can be either a denial of service, cache poisoning, or compromise of the target server.

DNS redirection (MITM) attack: DNS running over UDP is a stateless protocol, which makes it susceptible to man-in-the-middle (MITM) attacks. Examples of this type of attack include DNS changer, DNS replay, or illegitimate redirection attacks, and the primary motives behind them are hacktivism, phishing, website defacement or data stealing.

DNS tunneling: The name of this attack refers to using DNS as a covert channel to bypass traditional defense mechanisms. Outbound and inbound data being communicated are encoded into small chunks and fitted into DNS queries and DNS responses respectively. DNS is a very reliable yet fairly stealthy communication channel, and this makes DNS tunneling an attractive attack method to malware operators. Where other communication fails, the malware that lands on a victim host can contact its operator (aka Command and Control) and pass stolen data undetected, or fetch commands to be performed on the compromised host.

Domain phishing: This attack is an attempt to phish a legitimate domain to that of one controlled by hackers – often the domain of a financial institution or a travel agency, for example - and illegitimately acquire sensitive information such as usernames, passwords, social security numbers, PINs or credit card details. Once this sensitive information is gathered, the actual attack can then be performed.

DoS and DDoS attacks: The size, velocity and complexity of DoS and DDoS attacks grew significantly in 2012, although they consist mainly of two types:

1. Those attacks that target DNS infrastructure servers directly – such as ICMP/SYN/UDP/TCP flood attacks, land attacks, application-level floods, Smurf attacks. These also include botnet-triggered attacks that request recursion, spoof their source addresses and send large amount of DNS queries to choke specific DNS servers.

2. Those that use a DNS server to carry out the attack such as an amplification or reflective DDoS attack. In this scenario, the attacker uses spoofed DNS queries and causes the DNS server to send large, unsolicited DNS responses to target the victim machine. Small DNS queries are made to multiple DNS servers, and are likely to go undetected while generating massive DDoS attacks to the victim host by leveraging the amplification provided by DNS.

DNS fast fluxing: Fast fluxing refers to the rapid changing, swapping in and out, of IP addresses with extremely high frequency through changing DNS records with short-lived TTLs (time to live). Domain fluxing refers to the constant changing and allocation of multiple fully-qualified-domain-names (FQDNs) to a single IP address of the Command & Control (C&C) server. Bots that use dynamic algorithms to generate FQDNs each day, as the bot agent tries to locate the C&C infrastructure, are on the rise and are commonly referred to as Domain Generation Algorithm (DGA) bots.

Advanced Persistent Threats (APTs): APTs refer to attacks that gain unauthorized network access, remaining undetected for long periods. As their name suggests, APTs are

advanced malware, persistent in their nature, well funded, and entirely motivated to accomplish the specific goal for which they have been designed. Examples of APTs include Torpig, Kraken, or the most recent TDSS/TLD4 malware – all of which leverage DNS to stealthily communicate with a remote C&C server to gather additional malware packages and instructions, and carry out their attacks.

As is clearly evident from the examples above, DNS attack vectors are far too wide and deep for one single technology to be able to stop all of them. Comprehensive protection of DNS infrastructure and services requires a multi-pronged security strategy that employs a layered defense using some or all of the following solutions:

DNS firewalls, inline devices that provide real-time threat intelligence, anomaly detection and protection against malicious domains.

DNSSEC, which digitally signs DNS records to ensure that no poisoning of the records can happen from untrusted sources.

DoS/DDoS protection systems that can detect and take protective action against advanced denial-of-service attacks.

Data leakage prevention (DLP) monitoring systems, which can detect if any data leakage is taking place using DNS, among other protocols.

Dedicated APT-aware analytics systems that employ machine learning along with other behavioral techniques to detect APT malware that use DNS to communicate with C&C servers.

Conclusion

DNS is fast becoming an attractive option for attackers and malware authors wishing to evade existing defense mechanisms and exploit any one of the aforementioned threat vectors, with a primary motive of cyber war, industrial espionage, hacktivism, political gain or protest, theft of data, distribution of SPAM, or to carry out a coordinated DDoS attack.

DNS-based attacks have been on a meteoric rise over the past year, which suggests that existing intrusion detection/prevention systems (IDS/IPS) and Next-Generation firewalls are no longer sufficient means of defense. It is clear that enterprises now need to consider a multi-pronged defense strategy as a means of combating these modern threats and the malware that reliably use DNS to evade existing defense mechanisms.

Srinivas Mantripragada is the Vice President of Technology at Infoblox (www.infoblox.com).



Want to reach a large audience of security professionals by writing for (IN)SECURE?

STOP

Send your idea to mzorz@net-security.org



Events around the world

RSA Conference 2013 Europe

www.rsaconference.com

Amsterdam RAI, Amsterdam, The Netherlands

29 October - 31 October 2013

Virus Bulletin 2013

www.virusbtn.com/conference

Maritim Berlin hotel, Berlin, Germany

2 October - 4 October 2013

HITBSecConf2013 - Malaysia

www.conference.hitb.org

Okura Hotel, Amsterdam, The Netherlands

14 October - 17 October 2013

2nd Annual Cyber Resilience for National Security

www.tinyurl.com/mgk43kb

DC/VA, USA

17 September - 19 September 2013



2013

BERLIN 

2 - 4 October 2013

VB2013 BERLIN **2-4 OCTOBER 2013**

Join the VB team in Berlin, Germany for *the* anti-malware event of the year.


- What:
- Three full days of presentations by world-leading experts
 - Mobile malware
 - Banking trojans
 - Phishing & spam
 - Java exploits
 - AV testing
 - Pentesting
 - Law enforcement
 - Last-minute technical presentations
 - Networking opportunities
 - Full programme at www.virusbtn.com

Where: The Maritim Hotel Berlin

When: 2-4 October 2013

Price: \$1895 + VAT; VB subscriber rate \$1795 + VAT
10% early bird discount available until 15 June

BOOK ONLINE AT www.virusbtn.com

A person in a dark suit and blue tie is holding a glowing, translucent globe with a network of blue lines and dots. The background is blurred with blue and red light effects.

IT security jobs: What's in demand and how to meet it by Mirko Zorz

The information security job market continues to expand. In fact, according to a report by Burning Glass Technologies, over the past five years demand for cybersecurity professionals grew 3.5 times faster than that for other IT jobs.

To make things even more interesting for those looking to pursue a career in information security, the InformationWeek 2013 Salary Survey reports that 63% of IT security staffers are satisfied or very satisfied with all aspects of their jobs, while nearly two-thirds of IT security managers are similarly content. The demand for security pros is booming, so much so that the gender gap has nearly closed when it comes to pay. Employment in the occupational group that includes information security analysts is projected to grow 22 percent from 2010 to 2020, faster than the average for all occupations, according to Eric Presley, CTO at CareerBuilder.

So, let's say you want a career in information security, where do you start? What credentials do you need? What are employers looking for? Read on to find some answers.

Knowledge

Most employers will definitely appreciate your formal education and certificates. "Being certi-

fied and part of a professional organization demonstrates that the individual is actively involved in keeping up to date with current developments in their chosen profession. Certification is proof that a candidate takes his or her professional development seriously and invests time and effort in furthering their skills and career," according to Allan Boardman, International VP of ISACA.

It's important to remember that the infosec industry differs from others in one very important aspect - the value placed on self-learning and improvement. While it's impossible to work as a doctor or lawyer without a degree, I know of many IT security professionals that are mostly self-taught, hold important positions and are respected in the community.

Remember that regardless of your educational background and shiny certifications, most companies will probably thoroughly test your knowledge for the job you're applying for. This is why those that excel in this industry are also those that are deeply passionate about their

field of expertise and continually educate themselves. They never stop learning and adapting to the threat landscape.

Networking

There are plenty of online resources you can use to network with other IT security aficionados. I would advise engaging on Twitter, updating your LinkedIn profile, keeping up with the latest news and participating in online forums.

If you're good with code, you can always contribute to an open source project. It's the perfect way to grow your network and you'll be able to put something tangible on your resume. Let's not forget some quality open source tools have been acquired and given a spotlight.

Allan Boardman comments: "I highly recommend joining a professional association such

as ISACA because the community of professionals and training opportunities will help the candidate do both. Soft skills are key because you can't just have technical skills if you want to succeed—you need to be a well-rounded professional with great communication skills and business savvy."

It's also recommended to lift your head from the monitor once in a while and engage with others in real-life. The world is full of information security conferences of all sizes that offer not only lectures but also hands-on workshops that can hone your skills. They are the perfect way to put a face to that Twitter handle and get to know people on a personal level.

Like any industry, information security is all about people and recommendations. You get more opportunities if people know who you are.

Like any industry, information security is all about people and recommendations. You get more opportunities if people know who you are.

Job hunting

If you follow IT security news, you'll see a lot of buzzwords being thrown around, but you're probably wondering what jobs are actually in demand vs. what company PR departments are spinning as the most important topic of the day.

Allan Boardman comments: "Security professionals need to be knowledgeable about the main threats and issues related to key current technology trends such as cloud services, social media, and consumerization of IT, including BYOD. They also need to be well-versed in data privacy and data protection, particularly if they are in financial services or health-care. It is highly desirable to have strong technical skills, including security architecture and forensics skills."

"Given the big data phenomena, data mining and business analytics skills are also very de-

sirable. Knowledge of protecting and securing SCADA systems for manufacturing and infrastructure are also important."

I also wanted to hear the perspective of CareerBuilder, a well-known online job site. Eric Presley told me: "Information security analyst positions are the most common job title you'll find, but relatedly, there's a large need for network architects and engineers with experience in managing security protocols. There's also a big push to digitize medical records in an efficient, compliant manner, and as a result, we're seeing increased demand for IT security professionals with experience in the health care space."

When searching for a job you can use a job board, ask your contacts on LinkedIn for help, but you can also use a headhunter. Wils Bell, President of SecurityHeadhunter.com offers some advice (IN)SECURE Magazine readers:

You may be happy in your current position at the moment, but you never know what might happen in the future.

"The vast majority of security talent is NOT visiting job boards, thus they never see the posted job. This is why so many cyber security jobs go unfilled for months, if filled at all. My search assignments always include direct 'cold call' recruiting, recruiting in my vast network of passive job seekers and of course a full search of my database when identifying potential security talent."

"Another benefit of a security headhunter search, over a job board ad, is potential security talented professionals are thoroughly and properly screened against the client job specs,

and the company culture, location, salary and so forth before a client presentation takes place. This process sure beats job board results," added Bell.

There's also another important thing to remember about job hunting. You may be happy in your current position at the moment, but you never know what might happen in the future. Bell advises on building a relationship with a headhunter even if you're not looking for a change. You never know what great career advancing opportunity might come across his desk in a year.

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



**DAILY OR WEEKLY
SECURITY NEWS
RIGHT IN YOUR INBOX**

net-security.org/infosecuritynews.php



Remote support and security: What you don't know can hurt you

by Nathan McNeill

A remote support solution is one of the most valuable tools a service desk technician can have in his or her arsenal. Rather than having to traipse to a user's desk (or sometimes fly or drive to another location) to see and diagnose a technology issue, remote access tools allow you to work on far away systems as if you were standing in front of them. Saving time, saving money – what more could you ask for?

In a word, security. The fact that these tools offer access and control over remote computers or systems means that they are enticing targets for hackers. For years remote access tools have been ranked as one of the top attack vectors for hackers; and that's a trend that's not going away.

In fact, the recent 2013 Verizon Data Breach Investigations report showed that for hacking-related breaches, desktop sharing or remote access services such as Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC) are the most common attack vectors for hackers that are motivated by financial gains such as accessing bank details. Trustwave's 2013 Global Security Report listed remote access as being responsible for 47 per cent of all the attacks that they analyzed.

For individuals that are targeted by hackers using consumer remote access tools, the standard advice given for keeping secure still stands: don't download any software or documents that are not from trusted sources, and be wary of attachments sent by email.

Companies like Microsoft don't and won't call you to let you know you have a virus on your machine, so just put the phone down on the scammers that try to convince otherwise and to install remote access software.

In the business world, there are other considerations to bear in mind. For organizations that run their own service desks and/or companies that provide tech support to customers, it's imperative that the remote access tools your own teams uses don't leave backdoors open to hackers.

Here are five things to consider on top of your traditional IT security precautions.

1. Examine the architecture of your remote support tool

With the growing number of remote workers, help desks are becoming increasingly reliant on remote access tools to support systems and devices that are not on the local network. However, the tools used to achieve this can be potential attack vectors themselves.

Older remote support products take a point-to-point approach, using a direct connection between one PC and another over the public Internet. By default, these point-to-point products don't work well through firewalls. In turn, this architecture encourages administrators to port forward traffic through their firewall and create listening ports that are accessible via the Internet.

While this makes it easier for the support team to fix problems for remote users, it does raise additional issues as well. For example, hackers

can find these open ports through a simple Internet scan, which is why they have become such a popular attack pathway.

For a percentage of these Internet-facing remote access ports, the administrator may have forgotten to change the credentials required for remote access from the default settings. If this is the case (and it often is), an attacker can slip right through the firewall. Even if the default passwords have been changed, these details should be changed on a regular basis and one should avoid dictionary terms so that attackers cannot successfully crack passwords.

To solve this problem, consider switching to a remote support solution that doesn't require open listening ports. At the very least, move away from default settings and passwords, and change passwords on a regular basis. No matter what solution you use, regularly review your system's log files to track any use of remote access tools by both end users and the IT support team.

BLACK AND WHITE. ON OR OFF. MANY OLDER REMOTE ACCESS SOLUTIONS HAVE BINARY ACCESS, SO ONCE YOU'RE IN, YOU'RE IN.

2. Make sure you can track who is doing what

Within many support teams, staff members don't require to use remote access tools all the time, for example when they're doing password resets. For this reason, it's often financially advantageous for technicians to share licenses. Unfortunately, many remote support tools only offer named-seat licensing models, where each license has to be tied to a single person's name/account. This results in the use of shared passwords and/or default login credentials, e.g. "tech1, tech2" type user names, to save funds for other tasks.

When licenses are shared it becomes nearly impossible to audit who did what to which systems via remote access, as there is no direct link between the support rep and the action that took place. If it does make financial sense to share licenses, then look at a remote access solution that allows concurrency of

license use but still requires individual logins and passwords.

Also, link remote support logins to your master identity management directories (e.g. Active Directory) if possible. This makes it much easier to centrally manage system access by teams and individuals, and activate and deactivate logins as technicians turn over.

3. Determine the type of system access controls you have in place

Black and white. On or off. Many older remote access solutions have binary access, so once you're in, you're in. Either you have full access to every system on your network and everything on those end systems, or you don't have access at all. As convenient and as easy as this may sound, if any default login credentials fall into the wrong hands, this all-or-nothing access can be the IT department's worst nightmare.

Your remote access solution should instead allow you to be more granular about what support staff have access to and what they are allowed to do. You should be able to restrict what systems or functions can be accessed by a team or an individual. This is particularly important for organizations that outsource all or some of their IT support. By putting more granularly permissions in place, the IT organization can securely allow vendors or partners to access only certain systems and monitor everything they do.

4. Record all actions taken during support sessions

Because remote access tools can allow technicians to make changes to unattended computers, it's important to have a precise audit trail of what takes place at any given time. For company IT teams, providing these records is essential as it demonstrates that best practices are being followed. If a session is not recorded, then it can be a good indicator that problems might be taking place, either in terms of support policies not being followed or an attack going on.

Audits for remote support involve having on file exactly what happens in each support session, such as chat transcripts and copies of all files transferred. This audit feature is often non-existent among legacy products. With nothing in the middle of a point-to-point connection, remote control sessions slip away in the night (or day) without any record that they ever took place. This is very convenient for hackers, so putting the right audit policy into action is essential for identifying and stopping potential attacks.

5. Standardize your approach

No matter what remote support solution you choose, there is great benefit to choosing a single solution.

For one, it is much easier to track and audit remote access when only one tool is being

used. If every rep is using their own set of tools, then monitoring and auditing their actions is much harder. This is also an issue when someone leaves the organization: if they have individual remote access tools set up; who manages them after they depart and how do you ensure the former employee no longer has access to your systems?

This is not just a theoretical problem: at one consulting and financial services company we found 17 different remote support tools in place across the organization, many of which the management team were unaware of. Mandating the use of a central, consolidated solution can therefore stop unknown security holes from developing.

The second issue is around the sheer number of platforms that have to be supported. Using a mix of tools means that the staff members within the support function might not be able to access some platforms, such as Android, iOS or Macs, while others are. If this is the case, then the support team as a whole cannot provide the level of service that is required. Even without the security consideration, this would have an impact on the ability to offer good customer service.

Cutting down on the number of tools that are used is therefore good for both service and security improvements. Users get the same quality of service from all the support representatives that they might interact with, while the business can be sure that the tools used to provide remote access are secure.

The growth of mobile workers and BYOD has had an impact on how service desks and security professionals approach remote access. For companies with staff that are mobile, remote access is a vital and necessary tool to keep those users happy and productive. However, this does not mean losing control over security for those assets. Instead, the helpdesk will simply have to evolve its processes and tools to keep up with employees and customers and stay ahead of hackers.

Nathan McNeill is Co-founder and Chief Strategy Officer at Bomgar (www.bomgar.com). He is responsible for aligning Bomgar's long-term product strategy with the needs of its 6,500 customers. McNeill is active as an evangelist for the remote support market and speaks at many industry events, including TSIA, HDI, the Service Desk and IT Support Show, and CIO Synergy.



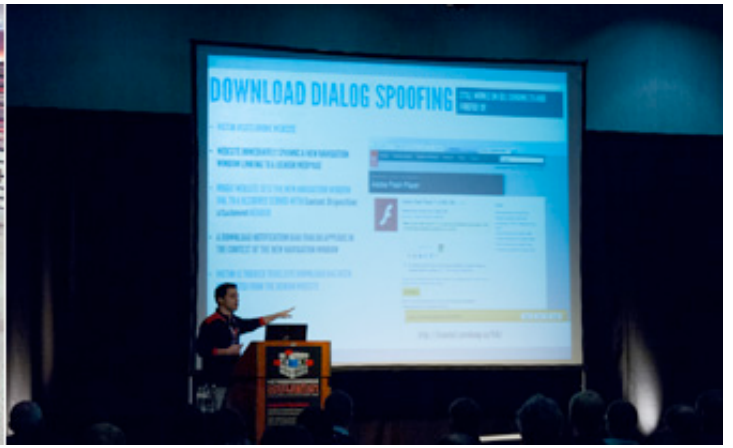
A closer look at HITBSecConf 2013 Amsterdam

Photos © #HITB2013AMS

The 4th annual HITB Security Conference featured keynotes by Edward Schwartz, Chief Information Security Officer at EMC / RSA and Bob Lord, Director of Information Security at Twitter.

The event also featured cutting edge attack and defense research including a presentation on the inner workings of the iOS 6.1 Evasi0n jailbreak presented by members of the world famous Evad3rs Team, a brand new kernel level exploit affecting Windows and even a presentation on remotely hacking airplanes.





Capture The Flag competition in full swing.





Bob Lord, Director of Information Security at Twitter.



Jim Manico, VP Security Architecture, WhiteHat Security.

HELP NET SECURITY

www.net-security.org

14 years of information security news

