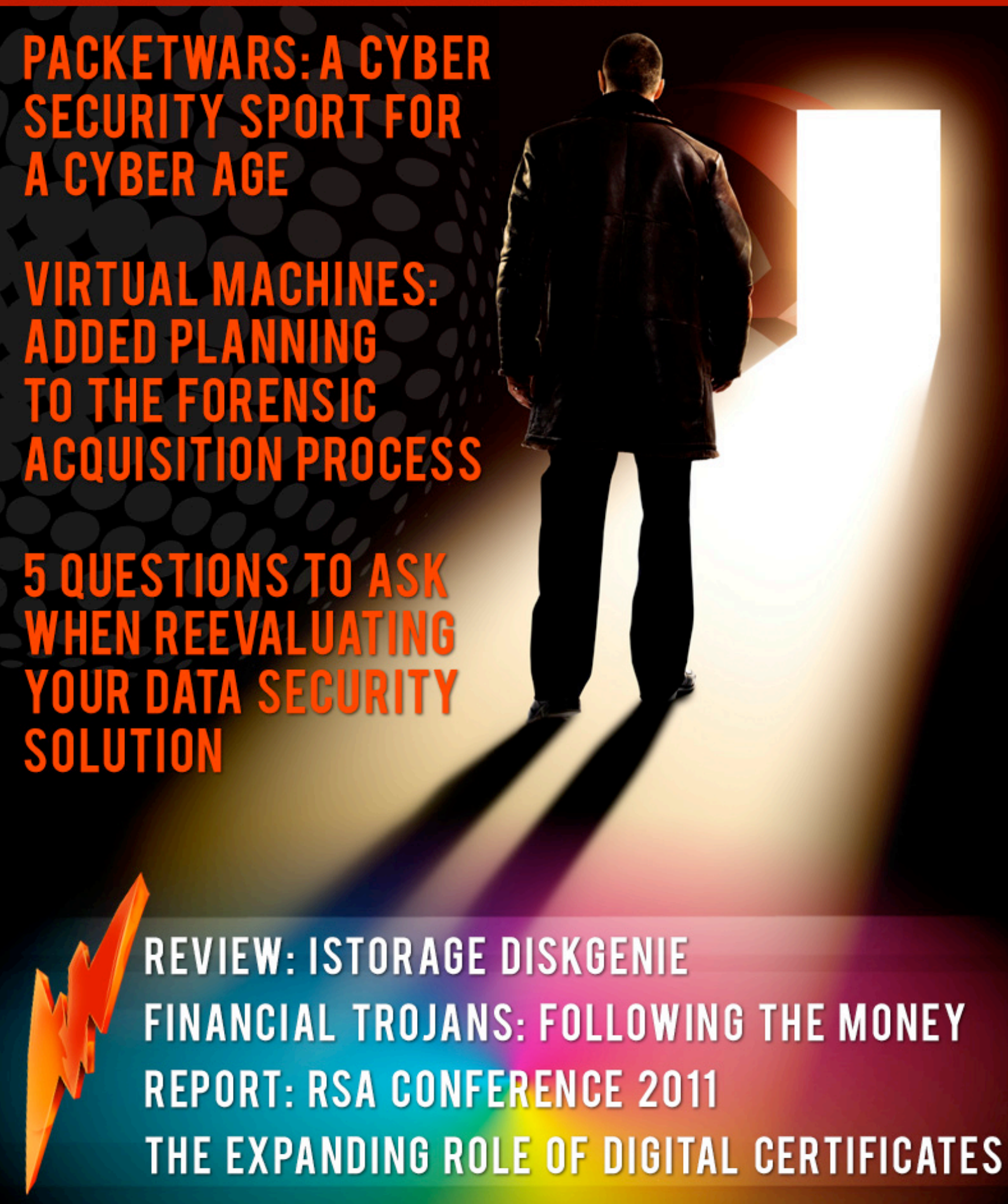
# [IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 29 - March 2011

## PACKETWARS: A CYBER SECURITY SPORT FOR A CYBER AGE

## VIRTUAL MACHINES: ADDED PLANNING TO THE FORENSIC ACQUISITION PROCESS

## 5 QUESTIONS TO ASK WHEN REEVALUATING YOUR DATA SECURITY SOLUTION



REVIEW: ISTORAGE DISKGENIE

FINANCIAL TROJANS: FOLLOWING THE MONEY

REPORT: RSA CONFERENCE 2011

THE EXPANDING ROLE OF DIGITAL CERTIFICATES

Entrust® Securing Digital Identities & Information

# <Let's Talk Enterprise Authentication

## Strong authentication. For a stronger enterprise.

**Entrust understands.** Organizations strive to be fully aware of the individuals and devices accessing resources, networks and facilities. And whether required by internal policy, industry mandates or government regulations, safeguards are needed to protect these critical assets.

**Going versatile.** When implementing strong authentication across an enterprise, it's important to recognize not all users and transactions require the same level of strong authentication. Entrust's versatile authentication platform is a proven solution for all enterprise environments — cost-effective and simple for end-users — and supports the variable demands of the enterprise market.

### < Versatile Authentication Platform
### < Physical & Logical Access
### < All Authenticators, One Solution

**The Entrust approach.** Entrust IdentityGuard is the most versatile authentication platform available. Core to Entrust's identity-based security approach, the platform boasts more authenticators than any other solution available today. And its flexibility helps evolve as technology and security objectives evolve over time.

**Let's talk.** Visit **entrust.com/enterprise-authentication** to discover how Entrust's proven approach can complement your existing enterprise authentication solutions.

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

# TABLE OF CONTENTS

## Welcome to (IN)SECURE 29
## the digital security magazine

The biggest security event of the year - I'm talking, of course, about the RSA Conference that was held in San Francisco in February - has been an outstanding success that we have witnessed first-hand.

The information and computer security market is alive and doing great, and it was a pleasure - as always - to see old friends and meet new ones which, until then, were mostly catalogued in our minds as a collection of Twitter avatars.

To make things even more interesting, we got an invite from the producers of the Dr. Phil show to talk about identity theft. We're located in Europe so it wasn't doable, but I bet it would have been quite the experience.

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, News Editor - zzorz@net-security.org
Marketing: Berislav Kucan, Director of Marketing - bkucan@net-security.org

### Distribution


## Growing focus on endpoint security

90% of business leaders are investing in resources to better manage the security of their endpoints, including servers, PCs and laptops, according to IBM. Over half of those surveyed are also extending security to smartphones and other instrumented devices, with plans to increase spending in this area. (www.net-security.org/secworld.php?id=10684)

## Secure containment solution for malware analysis

SRA Cyberlock is a highly secure appliance that enables enterprise IT organizations to automate and expedite the processes of analyzing malware behavior and responding to malicious network activities. Developed in conjunction with GFI Software, SRA cyber operations and forensics specialists have engineered Cyberlock to securely operate within existing network security infrastructures utilizing a virtual containment service. (www.net-security.org/secworld.php?id=10610)


## Phishers exploit New Zealand earthquake

Natural disasters are practically always exploited by scammers, and the earthquake that hit New Zealand and left thousands of its citizens homeless is not an exception. This time the scammers turned out a rather well executed phishing page that spoofs the legitimate New Zealand Red Cross website. (www.net-security.org/secworld.php?id=10685)

## Stolen e-mails reveal Morgan Stanley was hit by Aurora attacks

Global financial services firm Morgan Stanley seems also to have been a victim of the hackers behind the Aurora attacks which came to light a year ago when Google decided to go public with the information that their networks have been breached. Speculation about which companies have been targeted abounded, but this is the first time that Morgan Stanley was specifically mentioned, and that particular piece of information was found among the company e-mails stolen from HBGary and published online by Anonymous. (www.net-security.org/secworld.php?id=10679)

## Entrust credentialing services smartcards earn Microsoft certification


Entrust credentialing services and related smartcard technology have earned full Microsoft certification for demonstrating hardware compatibility with the company's line of operating systems. This ensures customers, partners, enterprises and vendors that the smartcards deployed with Entrust's SaaS credentialing platform are compliant with Microsoft Windows. (www.net-security.org/secworld.php?id=10649)

## Information security pros stretched thin and overworked

An (ISC)2 study says new threats stemming from mobile devices, the cloud, social networking and insecure applications, as well as added responsibilities such as addressing the security concerns of customers, have led to information security professionals being stretched thin, and like a series of small leaks in a dam, the current overworked workforce may be showing signs of strain. (www.net-security.org/secworld.php?id=10630)

## One in 10 IT pros have access to accounts from previous jobs

According to a survey that examines how IT professionals and employees view the use of policies and technologies to manage and protect users' electronic identities, the sharing of work log-ins and passwords between co-workers is a regular occurrence. The results of the survey underscore how these technologies, or lack thereof, are making it more difficult for employees to get their jobs done, and how they are causing greater concern about insider threats to IT security. (www.net-security.org/secworld.php?id=10620)

## 70% of SMS spam is financial fraud


An analysis of SMS traffic conducted from March through December 2010 reveals that according to the reports of misuse submitted by AT&T, Bell Mobility, KT, Korean Internet & Security Agency, SFR, Sprint, and Vodafone consumers, spam is found across all networks, and at levels higher than originally anticipated. The reports were collected by the pilot of the GSMA Spam Reporting Service (SRS), which identified and aggregated reports submitted by users via a short code. (www.net-security.org/secworld.php?id=10614)

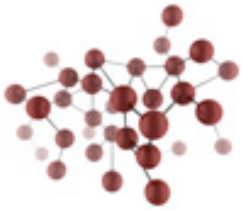
## The Spam King is free again, claims his spamming days are over

Robert Soloway, one of the most prolific spammers whose activities earned him the nickname Spam King, has been released from prison after a little less than 4 years inside. He is allowed to go back online, but according to his plea deal, probation officers will monitor his e-mail correspondence and which websites he visits for the next three years. (www.net-security.org/secworld.php?id=10698)

## SANS Secure Europe: In-depth information security training

SANS Secure Europe Amsterdam is the second biggest event outside of the US offering 8 top level courses. What makes this a unique event is that these classes run over two weeks, with 4 each week, giving you a chance to make the most of your travel budget and build your knowledge with two classes, one after the other. (www.net-security.org/secworld.php?id=10690)

## Top 10 botnets of 2010



Damballa's Top 10 Botnet Threat Report shows a dramatic increase in Internet crime and targeted botnet attacks. At its peak in 2010, the total number of unique botnet victims grew by 654 percent, with an average incremental growth of eight percent per week. The report reveals that many new botnets were discovered in 2010. (www.net-security.org/secworld.php?id=10603)

## iPhones and iPads reveal passwords regardless of passcode protection

Losing your iPhone or iPad equals having your passwords compromised - even if the device is protected with a passcode. The results of an experiment conducted by Jens Heider and Matthias Boll, two researchers from the Fraunhofer Institute for Secure Information Technology, have proven that the combination of a modified jailbreaking technique and the installation of an SSH server on a device running iOS results in a complete circumvention of the passcode. (www.net-security.org/secworld.php?id=10570)

## Internet fraudsters jailed for online criminal forum


A group of young internet fraudsters who set up an online criminal forum which traded unlawfully obtained credit card details and tools to commit computer offences were jailed for a total of 15 and half years. All pleaded guilty. The gang are believed to have been responsible for the largest English-language online cyber crime forum and were all arrested on various dates in 2009 and 2010, following a complex investigation. An examination of the rebuilt forum and its database revealed many thousands of data entries relating to individuals' personal details including names, dates of birth, bank details, passwords, PayPal accounts and social security numbers. (www.net-security.org/secworld.php?id=10696)

## Researcher offers free voice and text encryption app to Egyptians

The explosive situation in Egypt has mobilized many repression-hating individuals in the world to try to do something to support the country's citizens in their efforts to down the government and president Mubarak. The last ones to join the fray is well-known security researcher Moxie Marlinspike and his team at Whisper Systems. (www.net-security.org/secworld.php?id=10579)

## 2-step authentication finally available to Google's non-paying customers

Google's corporate users have had the option of using two-factor (two-step) authentication for nearly five months now, and the time has finally come for non-paying customers to receive the same option. The feature will be opt-in and to set it up, users should go to their Account Settings page and click on the "Use 2-step verification" link in the Security section.
(www.net-security.org/secworld.php?id=10576)

## HBGary breach revelations and repercussions

Anonymous downed HBGary's website and breached its networks, downloading a serious amount of confidential information (e-mails, malware data, financial data, PBX systems) belonging to the enterprise and publishing some of it. The e-mails reveal that the claim that started it all was actually not a threat against Anonymous, but a way to get them to start a feud that would bring more attention to Barr's work, his scheduled speech at the B-Sides Conference about his results and, finally, to the problem of Anonymous attacks present for enterprises, which would, hopefully, be also good for HBGary and HBGary Federal.
(www.net-security.org/secworld.php?id=10572)

## Facebook survey scam toolkit lowers entry bar for scammers


If you have been wondering about the recent proliferation of survey scams on Facebook and thinking to yourself how is it possible that so many people to know how to develop these scammy applications, the answer is actually really simple: there is a Facebook viral application toolkit for sale on the Internet, and it costs merely $25.
(www.net-security.org/secworld.php?id=10562)

## 73% of organizations hacked in the last 2 years

Website attacks are the biggest concern for companies, yet 88 percent spend more on coffee than securing Web applications, according to a survey by Barracuda Networks, Cenzic and the Ponemon Institute. According to 74 percent of respondents, Web application security is either more critical or equally critical to other security issues faced by their organizations. Despite this, the study shows there are many misconceptions around the methods used to secure Web applications, primarily Web application firewalls and vulnerability assessment.
(www.net-security.org/secworld.php?id=10550)

## Increasing adoption of open source software

A recent survey by Gartner found that more than half of organizations surveyed have adopted open source software (OSS) solutions as part of their IT strategy. Nearly one-third of respondents cited benefits of flexibility, increased innovation, shorter development times and faster procurement processes as reasons for adopting OSS solutions. However, the survey revealed that only one-third of responding organizations had a formal OSS policy in place. (www.net-security.org/secworld.php?id=10545)

## USB autorun attacks against Linux

Many people think that Linux is immune to the type of Autorun attacks that have plagued Windows systems with malware over the years. However, there have been many advances in the usability of Linux as a desktop OS - including the addition of features that can allow Autorun attacks. This Shmoocon presentation by Jon Larimer from IBM X-Force starts off with a definition of autorun vulnerabilities and some examples from Windows, then jumps straight into the Linux side of things. (www.net-security.org/secworld.php?id=10544)

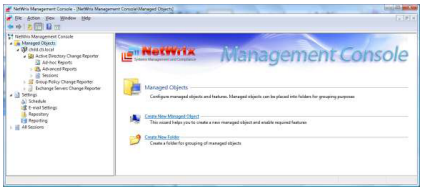
## Hackers compromised Nasdaq's network

Hackers continue to breach systems of vital importance to the US, and the latest one to be compromised is the one belonging to the company that operates the Nasdaq Stock Market. And even though people familiar with the investigation into the matter - mounted by the Secret Service and the FBI - say that the actual trading platform was not compromised, it is worrying that so far it has failed to explain what the attackers were looking for. (www.net-security.org/secworld.php?id=10538)

## Private info on Facebook increasingly used in court

Making the content of your Facebook account private can thwart the social network's plan to share as much information possible with advertisers, but may not keep out lawyers looking for material that will contradict your statements in a court of law. US lawyers have been trying to gain the permission to access the private parts of social network accounts for a while now, but it seems that only lately they have begun to be successful in their attempts. (www.net-security.org/secworld.php?id=10524)

## New version of NetWrix Change Reporter Suite




NetWrix recently released the newest version of NetWrix Change Reporter Suite, the integrated change auditing and compliance solution that provides a streamlined approach to IT infrastructure auditing. The newest edition includes enhanced reporting capabilities, and now tracks all changes made to Active Directory, Group Policy, virtual machines, MS Exchange, SQL Server, file server and appliances, Windows servers, SharePoint and network devices. (www.netwrix.com)

# Virtual machines: Added planning to the forensic acquisition process

by Megan Bell and Kai Lintumaa

**What happens when your organization experiences a security breach or receives a subpoena for electronic evidence and virtual machines (VMs) are involved? As this scenario becomes more common, it may not be sufficient to image a powered-down hard drive. And if the hard drive is imaged, it may be questionable whether the procedure accounted for the all evidence required to analyze a VM. This article presents a set of issues to consider when preparing for forensic acquisition of a VM.**

## VM described in this article

A VM is software (set of files) that functions as a computer without physically being a computer. A VM may also be called a VM container. A VM contains code that functions as a hardware layer, allowing a VM to operate independently of a specific hardware configuration.

A VM also has a fully-functioning operating system that enables a VM to be configured with all the features of a desktop computer. VMs may exist on a user's local computer, an external flash drive, a remote server or another computer that is not a server. The location of a VM is called the host.

In the case of forensic acquisition, a VM is one computer requiring imaging. When a VM's host computer is available for imaging, the VM and the host computer's hard drive represent two separate forensic acquisitions.

### Issue 1: There may be less evidence available in a VM collection than what is acquired in a non-VM forensics data collection.

Imaging a computer's hard drive traditionally involves making a bit-by-bit copy without the imaging process "touching" the electronic evidence—meaning no trace of the imaging process exists on the computer hard drive. This locks down the electronically stored information and maintains the integrity of metatdata such as file creation dates.

Evidence such as deleted files and records of recent user activity (e.g., usernames and password in the registry) may be present for analysis. This type of evidence may not be available in the forensic acquisition of a VM.

Consider the case of a VM hosted on a third-party remote server where a user logs in using Microsoft Terminal Services and roaming profiles are enabled.

As the user connects to a VM with Terminal Services, the user's profile is loaded into the VM. When the user disconnects from the VM, the user's profile is transferred to the roaming profile server.

In the event a VM's host server is unavailable to image (along with all other servers involved in supporting the VM), then the set of available evidence may be limited to the files that create the VM. If files such as temporary files are stored outside the VM, they may be deleted after a user's VM session is completed. Furthermore, unless a VM's host computer logs are available, additional data such as user login time and session activity may be unavailable.

Cloud computing has expanded the opportunity for hosting VMs in offsite data centers. Conducting a review of the VM's host environment and available data before acquisition is critical to understanding the availability of possible evidence.

The evidence in a VM collection may be more than the VM container on a host machine. Depending on the facts of litigation, there may be evidence in other areas.

### Issue 2: The body of evidence for a VM includes more than the set of files that constitute a VM.

A VM can run locally on a user's computer or a networked computer separate from a user's computer. The implication is that evidence may exist outside the VM, and that it may be worthwhile to collect related external evidence as part of a forensics acquisition.

Consider the case where each user in a group has a VM in the same network domain, and the VMs are not isolated from one another with security protocols. If one user's VM is the subject of a forensic acquisition and it is determined the user's VM has a strong history of interactions with other VM's in the same domain, the scope of evidence for collection may include:

- Several VMs
- The host system's logs
- Any sources of cached files.

Furthermore, if a user's profile is stored on another server, then it may be necessary to acquire evidence from multiple servers in order to build the appropriate body of evidence for preservation and analysis.

When considering the data collection of a VM, one needs to consider collecting the backups of the VM and the host machine. If a VM is backed up on a recurring basis, then a set of backups could show differences in files and user activity across time. For example, forensic analysis of a set of VM backups could be used to evaluate a pattern of asset misappropriation if supporting documents were created and deleted over time.

### Issue 3: Powering down a computer to image a hard drive is standard forensic practice, but there are cases where live imaging is a better option.

Live acquisition occurs when a computer is imaged in its powered-on state. Similar to imaging a powered-down hard drive, it captures all information that is saved on a hard drive at the time of imaging. Additionally, live acquisition captures information about software in use and current user activity—information missing from powered-down computers.

Live acquisition is also noted for its ability to capture volatile memory—data temporarily stored for processing. (Live acquisition of a VM is the same as a hard drive in that a VM is imaged in its powered-on state.)

Another reason to consider live acquisition is when a hard drive, VM or both are encrypted. Encrypted drives or VMs that are powered down for imaging may result in inaccessible forensic images if passwords are unknown or incorrect.

**Issue 4: VMs in distributed environments may need different forensic acquisition tools and protocols.**

Although forensic imaging of VMs is hardly novel, the scientific body of knowledge and best practices regarding forensic data collection of VMs is nascent in comparison to traditional forensic imaging practices. Part of the reason is the rapid adoption of virtualization technology over the past decade as broadband technology has matured.

The architecture underlying VM hosting and storage has changed how data is accessed, processed and stored. Accordingly, computer forensic data collection protocols and tools must be adjusted to accommodate the technological changes brought about by VM.

As an example, a VM can be hosted on a remote server that exists in an isolated domain with other VMs. The server has a specific port designated for intra-domain VM communications. However, the server has stricter rules and privileges for VMs communicating outside their native domain. All VM communications are tracked separately on a logs management server, and no logs are stored locally.

Furthermore, files contained within each VM are stored on a separate file server and file metadata such as creation date is stored on yet another server. Depending on the scope of forensic acquisition, a VM existing in this highly decentralized environment could necessitate a highly customized forensic acquisition.

This includes appropriate training on what constitutes the appropriate body of evidence for collection whether it's a single VM or a set of VMs. Furthermore, the forensic tool or tools used to support data collection in a distributed environment must be vetted so that the tools do not "spoil" the data being collected.

**Working with an organization's IT staff in advance of performing data acquisition will improve the overall success of forensic acquisition within an agile environment.**

**Issue 5: VMs in distributed environments may create additional acquisition challenges such as identifying a VM's current server location as well as the location of its related files and data sources.**

The evolution of "agile" computing presents additional challenges in forensic acquisition of VMs. In an "agile" computing environment, VMs and other data move from server to server over time to balance server load and resources. Locating a VM may take time and forensic acquisition may need to account for a VM in transit between servers.

Access to server logs over a period of time may be limited if the logs no longer exist.

Working with an organization's IT staff in advance of performing data acquisition will improve the overall success of forensic acquisition within an agile environment.

**Issue 6: Additional steps may be required to establish the correct timeline for a VM user.**

When a user has the capacity to access a VM from a remote environment, forensic investigators must establish and corroborate the correct time zone for the user. If a user has a designated computer, imaging the user's computer may provide sufficient evidence to build a timeline for a user's activity.

When this is not possible, more traditional investigative methods may be required to establish a user's whereabouts. For example, in-person interviews, network access logs or card-reader logs may be required to corroborate a user's location and activities.

A VM's source for date and time also requires verification as it depends on how the VM is configured. If a VM resides on a single computer, then the host computer's system clock is most likely responsible for establishing date and time. If a VM is part of a larger network configuration, then the time may be derived from a specifically organized domain of VMs or from a time management server.

## VM forensic acquisition: Success depends on knowledge and teamwork

As organizations continue to expand the use of VM technology and outsource their VM environments, the key to successful forensic acquisition of a VM's electronic evidence is the relationship between those involved in an investigation and IT professionals with knowledge of the specific VM environment. Among the factors that are important best practices for IT is to fully document usage of VMs, VM and host computer locations, and relevant configurations. Trying to assemble this information (crucial for forensic analysis) after the fact can be an almost impossible undertaking.

Megan Bell, Director of Analysis, and Kai Lintumaa, Senior Forensics Investigator, work at Kivu Consulting (www.kivuconsulting.com). Kivu combines technical and legal experience to offer investigative, data breach, and computer forensic analysis services to clients worldwide. Kivu Consulting is a licensed California private investigation firm and compliant with HHS Business Associate requirements.

# SANS Secure Europe 2011

## AMSTERDAM

THE MOST TRUSTED NAME FOR INFORMATION AND SOFTWARE SECURITY

## Eight of the best InfoSec training courses over two weeks in the heart of Amsterdam!

9 - 21 May 2011

### Week 1: 9-14 May

**SEC401: SANS Security Essentials Bootcamp Style**

**SEC540: VoIP Security**
*The only time this class is running in the EMEA region in 2011!*

**SEC560: Network Penetration Testing and Ethical Hacking**

**FOR508: Advanced Computer Forensic Analysis and Incident Response**

### Week 2: 16-21 May

**AUD507: Auditing Networks, Perimeters and Systems**

**SEC617: Wireless Ethical Hacking, Penetration Testing, and Defences**
*The only time this class is running in the EMEA region in 2011!*

**SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking**

**FOR558: Network Forensics**

**Venue:**
Radisson Blu Hotel, Amsterdam

**Register at:**
www.sans.org/secure-amsterdam-2011

**Contact:**
emea@sans.org

GIAC Approved Training

www.sans.org/secure-amsterdam-2011


**iStorage is a provider of high performance and ultra secure portable data storage and security products. Their diskGenie range of portable encrypted hard drives with secure PIN code access comes in various sizes (250, 320, 500, 640 and 750 GB) and two types of encryption (128-bit and 256-bit AES hardware encryption). I had the opportunity to test drive the 250 GB diskGenie with 256-bit AES encryption.**

The iStorage diskGenie is a compact and portable USB hard drive that encrypts its contents on the fly. The only way to access the files stored in it is through a number pad similar to one used on ATMs - although the PIN is not restricted to four digits, but can be any 6-to-16 digit combination.

The disk is very versatile - it can be used on machines running Windows, Mac OS and Linux. When taken out of the box, the disk is pre-formatted in NTFS for Windows and can be used immediately - no additional software installation is required, and you don't have to have administrative rights on your machine to use it.

The LED light on the disk tells you what is currently happening with the disk. Plugged in for the first time, the light is red - meaning that the disk is inaccessible until you type in the default PIN and press the "Unlock" (unlocked padlock) button.

But, before you do this, I would recommend changing the PIN. It is very easy to do - just follow the steps enumerated in the quick start guide sheet that is packed alongside the disk.

First you press and hold the "0" and "Unlock" buttons together for a few seconds until the LED light flashes red. Then, you enter the default PIN and press the "Unlock" button. You'll know you have successfully accessed Admin Mode if the LED light turns blue.

Then you press press and hold the "9" and "Unlock" buttons together until the LED light flashes blue, and now is the time to enter your new PIN and press the "Unlock" button. But, be sure to save the PIN somewhere because

if you lose it or can't remember it, the contents of the disk are practically lost to you.

The LED light will flash green three times to indicate the PIN is stored. Re-enter it and press "Unlock" and you'll know the PIN was changed successfully if the LED stays solid green for 2 seconds. In the end, you need only to exit the Admin Mode by pressing the "Cancel" button until the LED turns red.

Now, you are ready to use the disk with your brand new PIN by simply typing it in and pressing "Unlock".

Once you do that, the disk is immediately accessible and shows up on the machine like any regular removable drive - and you treat it like such. Drag and drop the files you want to store in it, which are automatically encrypted on the fly. Once you dismount the drive or simply plug it out, it immediately reverts to its locked state.

I tried it on my Windows 7 Ultimate running machine with the Intel Core i5 CPU, and it worked flawlessly. Then I tried it on my iMac running OS X 10.6.6 with a 2.4 GHz Intel Core 2 Duo processor.

Once I plugged it in and entered the PIN, I realized that I can read the files on it and copy files from it without re-formatting the drive to a Mac compatible format. But, to be able to store files on it, I had to do just that.

It is a very simple procedure. Go to Applications/Utilities/Disk Utility, select the disk from the list of drive and volumes, click on the "Erase" tab, give the disk a name, select the volume format to use (the manufacturer recommends "Mac OS Extended (Journaled) and click on the "Erase" button.

The process is over in a few seconds, and you can now use the disk as it was meant to be used.

Seeing that the disk encrypts the files put in it on the fly, you might be inclined to think that the whole process takes somewhat longer than it would with a regular, non-encrypting disk. Actually, it doesn't.

As an example, it took 3 minutes to copy a 5.5 GB folder in it - I have regular removable drives that work slower than that.


Un-mounting the drive after you finished using it will make its contents inaccessible. Un-mounting the disk before disconnecting it is advisable, since sometimes you may find that the files stored on it have disappeared because of your failure to do so.

Unfortunately, if you change your mind and want to use it again, you have to unplug it and plug it into the machine again. I didn't care for that, since the USB ports are on the back of my computer and I had to get up each time to do it.

The integrated USB cable - which is definitely a boon for people like me who abhor too much clutter - could also be a little bit longer.

The disk is easy to use with a laptop, but if you use it on a desktop computer, you can find that the cable is simply too short to plug it in and position it on the top of the casing, and definitely awkward to use when changing the PIN. But, on the other hand, it's nothing an extension cable can't fix.


Also, at first glance, I thought I would miss a screen on which you see the status of the device while you set up the PIN or insert it. It turns out, the LED is more than enough, and the keys are hardy enough to make it entirely obvious whether you have pressed them or not.

In any case, if you entered the wrong PIN, you simply won't get access and are free to try again five more times. After the sixth incorrect attempt, you will have to disconnect and reconnect the drive before trying again. All in all, you have a hundred tries to get the number right - after that, the disk assumes it is being attacked and will destroy the encryption key and lock itself, rendering the data useless and requiring a total reset and reformat to redeploy it.

Setting aside those minor limitations, the disk worked flawlessly. It's extremely fast and very reliable if used properly. I have been using it for a few months and have yet to find a glitch in its performance. According to the manufacturer, the data stored on the drive cannot be accessed even if the hard drive is removed from its enclosure - you simply must know the PIN.

The disk is enclosed in a sturdy enclosure and is protected by a shock mounting system which - among other things - makes it perfect for transporting data. The PIN protection (and its limitations) and the hardware encryption means that the disk cannot be brute force attacked and is not vulnerable to keyloggers or to corruption of data by malware or viruses.

An additional benefit of this disk is that allows enrollment of up to ten unique user ID's and one administrator, making it ideal for business collaboration within corporate environments.

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


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

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

### @falconsview

Ben Tomhave - Senior Security Analyst at Gemini Security Solutions.
http://twitter.com/falconsview

### @digininja

Robin Wood - Senior Security Engineer at RadomStorm.
http://twitter.com/digininja

### @SteveD3

Steve Ragan - Reporter for The Tech Herald.
http://twitter.com/SteveD3

### @lcamtuf

Michal Zalewski - Security expert and book author.
http://twitter.com/lcamtuf


**One of the most common complaints information security professionals make is that their senior management does not understand or care about information security. Information security professionals lament the lack of senior management buy-in, budget, time and resources they are given to protect what is cited as one of an organization's most precious assets - its information.**

Why are those tasked with protecting that information finding it hard to get the appropriate senior management buy-in? The problem is all down to communications, or rather the lack of communication. Most people tasked with managing information security for an organization come from an IT or technology background. Paradoxically for professionals who pride themselves on working in an industry focusing on how to improve the flow of information and support better communication, we struggle and often fail to make the connection we require when to dealing with our peers or senior managers.

In the book “Men are From Mars and Women are from Venus”, the author John Gray advises couples to improve their relationship by recognizing and accepting the differences between men and women. He argues that men and women are as different to each other as beings are from separate planets. Once you accept and understand these differences it makes communication and interaction between the sexes much easier. In a similar vein, we need to accept that there are core differences between information security professionals and senior management and while we both want the same thing - to ensure the security of our information - we need to understand each other better in order to achieve that.

The first difference is that when the business talks about managing and securing information they see it as the sole responsibility of IT and not of the business. People within information security think that securing information is everybody’s responsibility, and not just of those within the IT and information security functions.

The second difference is that unless you are working in a technology start-up company, Senior Management does not care about technology. Their focus is on the core functions of the business to ensure the business survives, meets its goals and also on being accountable to the stakeholders.

Any activities outside of the core business functions are there to simply support the business. As a result, activities such as IT are often looked upon as a necessary evil and therefore as being a cost to the business. And yes, this view is still widely held despite the productivity and other advantages IT brings to the business.

Compounding this problem is that many IT professionals don't fully appreciate information security either and see it as an additional cost. Indeed, in some cases the IT department views information security as a hindrance to getting projects delivered on time, meeting SLA commitments and implementing new technologies.

The blame is not all on the business' side either. Many of us working within information security focus too much on the technology and not on the information we are tasked with protecting. Not only do we not focus on the information, but we often do not understand the business of the organization and how that impacts the context of the information.

Information security is not all about firewalls, Intrusion Detection Systems, anti-virus software or whatever the latest shiny gadget is.

It is also about ensuring the proper policies and procedures are in place and that people are trained and educated properly to understand their role and responsibilities in securing the information they deal with on a daily basis.

**Paradoxically for professionals who pride themselves on working in an industry focusing on how to improve the flow of information and support better communication, we struggle and often fail to make the connection we require when to dealing with our peers or senior managers.**

Information security professionals also do not talk to their business colleagues or to senior management in a language they understand. We tend to focus too much on the technical details rather than speaking in terms that business people can understand.

Telling a senior manager "there is a zero-day vulnerability which could grant an attacker root access to the database server" does not have the same impact as telling that same manager "a security weakness in the system could allow an attacker to download all our clients' credit card information".
Likewise, senior management doesn't care whether or not the spam filters use Bayesian analysis, Real Time Blocklists or the Sender Policy Framework, but they do care about how much time is wasted by staff having to delete spam e-mails.

This inability to understand each other can lead to frustration for both parties and lead to the business seeing information security at best as something that needs to be done in order to meet some compliance requirements, or at worst to be ignored completely.

So how do we solve our interplanetary communication problems and get both parties to better understand each other?

**Telling a senior manager "there is a zero-day vulnerability which could grant an attacker root access to the database server" does not have the same impact as telling that same manager "a security weakness in the system could allow an attacker to download all our clients' credit card information".**

Thankfully, this is not a mammoth task and a few simple steps can help you have a more meaningful and rewarding relationship with senior management:

• Realize that while senior management cares about information security, it does not necessarily care about it as much as you do. They have a lot of other responsibilities and demands on them, so you must understand that they may not be able to give you the attention and time that you think you deserve.

Once you understand that their interest in information security is limited, you need to be ready to take full advantage of whatever opportunities you may have to interact with them.

• Start off by getting a better and deeper understanding of the business requirements of your organization. Once you do that, you will be more able to align your information security program with the needs of the organization.

To do this you should review the organization's annual report - it will provide you with good background information into the organization and how it has performed in previous years against its stated goals. Get visibility of the organization's business plan for the coming years so that you can understand how it may impact on the information security requirements for the business. For example - Will the organization be moving into any new markets or geographical regions? Will it be outsourcing any of its services or using cloud computing? Any of the above business initiatives will have a major impact on your information security strategy.

• Meet more regularly with your peers and with senior management so that you can better understand their business requirements and the business challenges they face. While this can be something as formal as arranging regular meetings with your peers, it can also be done informally by meeting them for regular coffee or lunch breaks.

Regular contact with your peers will make you appear more approachable to them and as a result they should be more willing to discuss matters relating to information security with you. It will also provide you with early indications of any business initiatives that may need input from information security.

**FUD is often used to coerce the business into making a decision to purchase a solution by leveraging of the fear factor of what could happen should the business not take the recommended plan of action.**

• Remember that while you may find the technological challenges that your role brings you interesting, your colleagues may not find them as exciting. Using technical jargon, the latest buzzwords and the dreaded TLAs (Three Letter Acronyms) will quickly lead to a disinterested audience resulting in the key message you want to deliver being lost.

Management understands and speaks about issues relating to the business in terms of risk. Learning to understand risk and how to present it to the management will enable them to appreciate and better understand what you are trying to achieve.

Remember though that while they may better understand what you are proposing they may not agree with it. However, with this approach the business can better explain to you the reasons behind their decision and can better understand and accept the consequences of that decision.

• It is also wise not to use the Fear, Uncertainty and Doubt (FUD) approach to get buy-in for your ideas. FUD is often used to coerce the business into making a decision to purchase a solution by leveraging of the fear factor of what could happen should the business not take the recommended plan of action.

This often results in a solution being implemented for the wrong reason and without the full support of the business. When the dreaded event you warned the business about never happens you then become the "boy who cried wolf".

Inevitably this will make it much more difficult to convince management to agree to the next solution you wish to implement.

• Don't fall into the trap of being heard by the business only when something has gone wrong and security has been breached. This often results in the business equating information security to bad news. Lose this image by regularly publishing reports and statistics on the positive impact your initiatives are bringing. This need not be a major task as there are many sources of information that you can use, such as the percentage of spam e-mails blocked, the number of computer viruses prevented or how many password resets had to be carried out in the previous month.

Remember though to try and translate that information into something that is meaningful to the business. If you can present your reports in terms of cost savings, productivity increases or other metrics that are important to the business than your reports will provide a more positive image of information security to the business.

## Conclusion

As in all relationships, getting the communication right is key to making that relationship a success.

Taking the appropriate steps to improve the communication between information security and management can lead to a stronger and effective information security program.

It requires some hard work and understanding, but it does not mean you have to stop thinking senior management is from another planet. In fact, I encourage you to do so.

Brian Honan is the founder and head of Ireland's first Computer Emergency Response Team (CERT) team (www.iriss.ie), as well as owner of BH Consulting (bhconsulting.ie).


Secunia
Stay Secure
Reduce the window of opportunity
Why are end-points increasingly vulnerable to attacks?
Access the Secunia Yearly Report 2010 to:
• Understand the state of the security ecosystem
• View vulnerability data and trends
• Plot your optimal defence against vulnerabilities
Stay updated, stay secure.
Download Report:
http://secunia.com/company/yearly_report
Secunia.com


**In this day and (cyber)age, hacking contests are sprouting like mushrooms after the rain - and it's a good thing they do. For what better venue is there for exercising the offensive and defensive cyber skills of future "cyber warriors" than events such as these, where their talent can get noticed and appreciated, and inspire others?**

PacketWars differs somewhat from that formula. Its developers started it with an ambitious goal in mind - to educate people while having fun and to institute Internet's first cyber sport that is also spectator-friendly and offers a fertile ground for establishing local and global leagues.

## How the story began

"This is what we need," thought Bryan Fite (aka Angus Blitter), the developer of PacketWars, as he witnessed Ghetto Hackers' projection of a "geisha girl" commenting the gameplay at DefCon's Capture the Flag contest.

"In the mid-to-late 80's late me and my hacker crew HackSecKlan were attending any and all hacker conferences we could get to, and one of our favorite things about them was the various 'capture the flag' style games. We loved them," reminisces Fite. "But, as we saw it, there were downsides to having these contests during the conference."

He soon realized that anyone engaged in these contests would typically have to give up much of their social interaction time and missed presentations, and that most people who ran the games got burned out - whether it was because of the cost of organization or simply because it was a lot less fun to organize such events than participating in them.

Watching a variety of CTF events, he noticed that most hackers tried to attack the game platform instead of actually mastering the objectives.

He realized that the game platform should have two main characteristics: mobility and a design that couldn't or wouldn't be "hacked". But, the real turning point was the "geisha girl". "She was commenting on the game play. I was fascinated. It was so engaging. It sucked people in," he says. "In short - it was the key to making these events 'spectator friendly'".

And that became the last piece of the puzzle. In order to address all of the negative aspect of this contests, he decided that the answer was to turn CTF into a proper sport. "We needed a sustainable structure, that was fun to play, easy to execute and would hold the interest of those who weren't playing. And, with PacketWars, we think that we have accomplished this."

**PACKETWARS EVENTS CONSIST OF A SERIES OF "BATTLES" THAT PIT INDIVIDUAL PLAYERS OR TEAMS AGAINST EACH OTHER IN A RACE AGAINST TIME TO COMPLETE A NUMBER OF DEFINED OBJECTIVES**

## Inside PacketWars

PacketWars events consist of a series of "battles" that pit individual players or teams against each other in a race against time to complete a number of defined objectives. "Two of my favorite battles are "What's My Name?" and "King of the Hill", says Fite.

The first one is a straight up reconnaissance assignment - individuals or teams have a limited amount of time, normally 30 to 60 minutes, to "visit" numerous targets in a specified address space. They must record as many attributes about them as they can: OS, running services, versions, known vulnerabilities, etc. Whoever identifies the most accurate attributes in the shortest period of time wins the battle.

"'King of the Hill' is pure carnage!" recounts Fite. "Battles normally last 2 to 4 hours and create a 'Battle Space' within a specified address space (kill zone). The external attack surface is usually based on difficulty level of the battle and experience and skill level of the combatants.

However, once the outer layer of security has been breached, combatants can leverage compromised assets inside of the Battle Space to attack internal assets or even other combatants - just like in the real world."

Apart from being the developer, Fite is also "The Packet Master". He facilitates the battles and serves as a commentator by explaining the attacks to the spectators. "It's a throw back to old RPGs, when I played the role of Dungeon Master," he says with a smile.

To participate in a public PacketWars battle all you need is a computer of your own. The organizers sanction players and teams at their discretion, but there are currently no extra fees to pay other than admission to the hosting event - typically hacker and security conventions. Event sponsors pay for the operational costs of the battles and provide prizes.

Battles can be played by individuals and teams. It is assumed all players are law-abiding citizens, and illegal activity of any kind is not tolerated. "That mainly refers to physical attacks on others or on their equipment," he says. "In the real world, physical attacks are certainly an option, but in our simulations they are prohibited. Other than that, the battle unfolds on an isolated network, so pretty much everything else goes."

**BATTLES CAN BE PLAYED BY INDIVIDUALS AND TEAMS. IT IS ASSUMED ALL PLAYERS ARE LAW-ABIDING CITIZENS, AND ILLEGAL ACTIVITY OF ANY KIND IS NOT TOLERATED**

Typical PacketWars players are security and IT professionals, students, hobbyists, and the occasional hacker. "This is a very accessible sport for beginners. In the past I would say you had to have much more experience. When it comes to organizing teams, we suggest the players to think about covering a varied skill-set," explains Fite.

"TCP/IP and basic networking is probably the only real technological requirement. But you won't get far without good application and OS skills," he says.

"We have introduced a player rating system. The more you play - earning league points - the better we are at rating your skill levels. Registered players can accumulate league status and be eligible for special Battle opportunities, including invitational events not open to the public."

The basic idea is to get as many players possible involved, so that a lot of games can be played. Sometimes qualifying events are run or participation is limited due to physical constraints based on the battle venues, but other than that - everyone who intends to follow the rules is welcome.

"We try to hit as many events as possible," Fite explains. "However, we are constrained by time and budget. In order to get more coverage, we sanction some CTF games and run remote games. In addition, we have started building regional franchises. This builds local and global teams for league play - expanding the sport in a cost effective and sustainable way."

Private battles are also organized. The PacketWars platform is often used for training, team-building or QA/product testing sessions. It is a great environment for honing offensive and defensive computing skills and capabilities. Fite is of the opinion that PacketWars could create more and better "cyber warriors" in a shorter period of time than the current practices.

**AND PACKETWARS HAS THE POTENTIAL OF BEING NOT ONLY A FUN AND EDUCATIONAL EXPERIENCE FOR THE PLAYERS, BUT ALSO TO INSPIRE IN SPECTATORS A WISH TO LEARN MORE ABOUT THE TECHNIQUES USED AND ABOUT CYBER SECURITY IN GENERAL**

"We have players who work in government or law enforcement roles," he says. "I know of several people who have referenced their involvement with PacketWars on their CVs and still got hired. I like to think it is viewed as a positive indication of a candidates experience."

In this day and age when various government agencies around the world are trying to attract knowledgeable individuals that could defend the country's cyberspace if the need arises, I must say that I think he's right.

And PacketWars has the potential of being not only a fun and educational experience for the players, but also to inspire in spectators a wish to learn more about the techniques used and about cyber security in general. All Battles are recorded - audio, video and complete telemetry - and this content is presented to the public under a Creative Commons license.

"We are trying to expand the appeal outside of the current demographic. We want people to care about the players. So, we have experimented with different formats. Some at live events. Others post production," Fite explains their future plans. "We think the key to taking it to the next level is attracted a non-technical audience. After all, you don't have to drive fast to enjoy Formula One."

---

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


## InfoSec World Conference & Expo 2011

www.misti.com - Orlando. 19-21 April 2011.

## Infosecurity Europe 2011

www.infosec.co.uk - London. 19-21 April 2011.

## SANS Secure Europe Amsterdam 2011

www.sans.org/secure-amsterdam-2011 - Amsterdam. 9-21 May 2011.

## SOURCE Boston

www.sourceconference.com/boston - Boston. 20-22 April 2011.

---

### Hackito Ergo Sum 2011

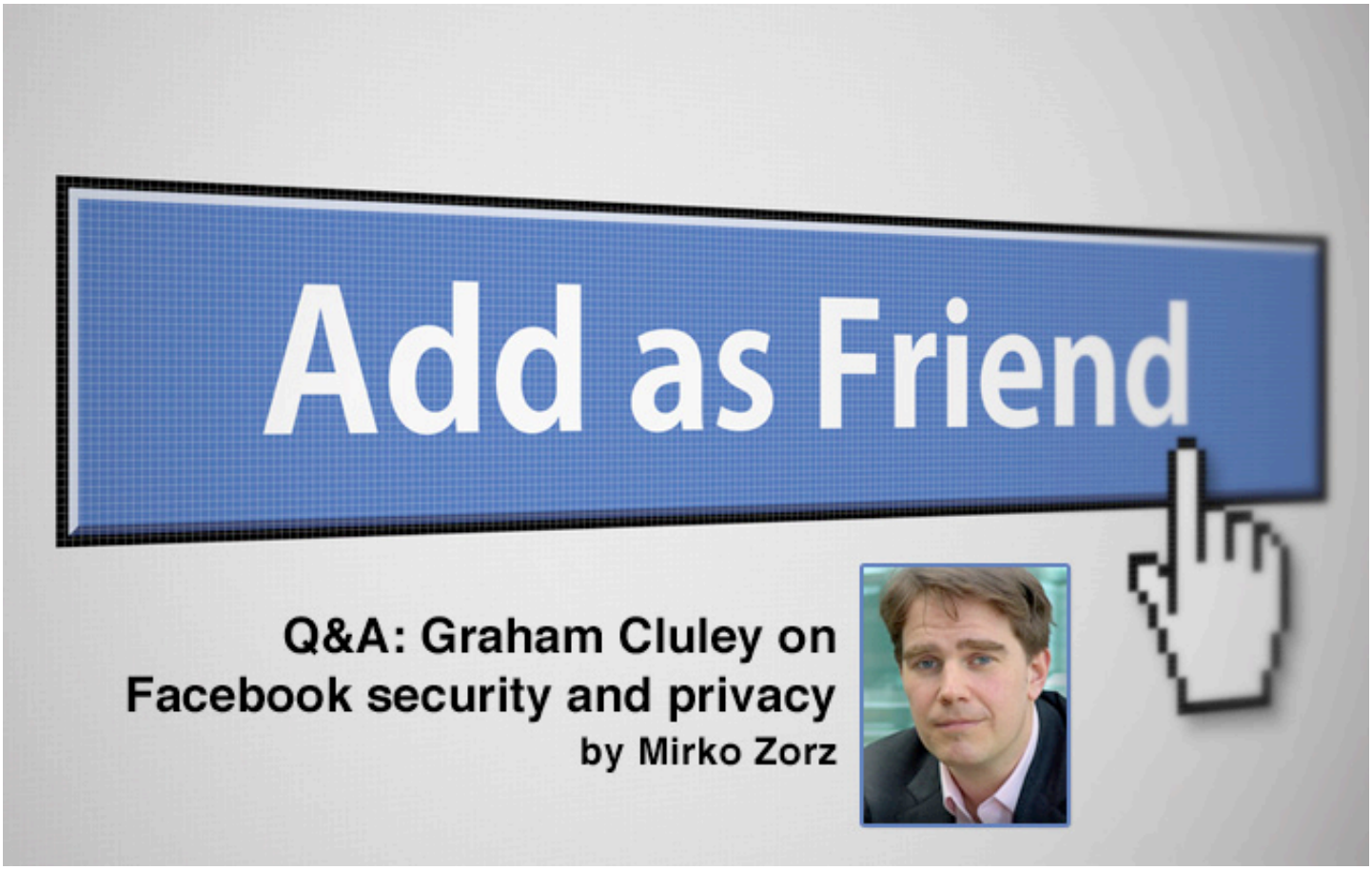
www.hackitoergosum.org - Paris. 7-9 April 2011.

### Infiltrate 2011

www.immunityinc.com/infiltrate.shtml - South Beach. 16-17 April 2011.

### CarolinaCon 2011

www.carolinacon.org - Raleigh. 29 April-1 May 2011.




**Graham Cluley is the senior technology consultant at Sophos and an expert on social networking security and privacy issues.**

**Should Facebook be doing more to protect the privacy of its users despite the fact such actions are in conflict with their advertising revenue? Do you believe that the constant privacy gaffes will eventually cost them one way or another?**

I like to think that there is a large number of people who would welcome a social network that kept them secure, and treated their privacy as a priority. I like to believe that if Facebook took a sea-change and decided to put its users privacy *first* (rather than the gradual erosion that has occurred) then they wouldn't find it would hit them in the pocket too much.

They may also find that they would be looked on kindly by regulatory and privacy bodies too.

Will their security and privacy gaffes hurt them in the long wrong? I'm doubtful.

I've encountered plenty of Facebook users who have had a bittersweet experience of rogue apps, stolen accounts, being spammed, etc, but still regularly login to the site. My guess is that they feel they *have* to be on Facebook to stay in touch with their friends - even if they don't always feel comfortable with it.

Think of it this way - what would have to happen for you to completely give up on the Web, or e-mail? You see.. it's not that easy... Facebook has users hooked.

**What features would a social networking site like Facebook have to have in order for you to be able to recommend it as a privacy-respecting service? Is it likely that such a service will ever exist?**

A privacy-respecting social network? It would need to give you complete control of every piece of your personal information, allowing you to specify who can and who can't view it. Furthermore, you would need to trust it not to erode your privacy by introducing new features that presumed you wanted to share info rather than not share info.

In other words, users should always have to opt in to sharing more information about

themselves, rather than opt out. In Facebook's specific case it needs to oversee third party applications much more closely to prevent abuse.

I'm not sure anything on the Internet can be 100% totally safe. This isn't just a Facebook problem. For instance, you might have a very well locked-down user profile but still have your Facebook password stolen by spyware on your PC.

**Is it possible to achieve a reasonable level of privacy while still using social networks? What practical advice would you give to those interested in protecting their information while still enjoying services like Facebook?**

The best advice is don't upload any information which you don't feel comfortable being broadcast from a loud hailer in the middle of Times Square.

I would say that you shouldn't feel obliged to tell the truth when you fill in your profile on social networks. For instance, why should you tell it your real phone number, address, etc? Many people feel compelled to tell the truth even when they're not required to and this can lead to awkward data losses later.

Unfortunately, Facebook's terms and conditions prohibit users from lying about themselves and their personal data. So, if you don't want to break Facebook's ToS but *do* want to use erroneous information on your profile to protect your privacy, you will have to leave the service.

**Many employees use social networking sites carelessly and are guilty of thoughtless information dissemination which can pose a security threat to the organization they work for. Are we nearing a point where access to such sites and the type of information disclosed is going to be part of a work contract?**

We see that most companies today are loosening up about Facebook. A few years ago, many firms blocked Facebook for productivity reasons. Now many businesses allow access to Facebook as they see it as an important part of their marketing and social media campaigns. And I think that's right - after all, you can bet your bottom dollar that your rivals are on Facebook, and why should you be at a competitive disadvantage?

Facebook can help your company get closer to its intended customers, and that's a great thing. But you do need to ensure that you act responsibly on it, and that you do not share inappropriate corporate information that may endanger your firm.

**While discussing Facebook at the RSA Conference in London, Bruce Schneier was very upfront and said: "These CEOs are deliberately killing privacy. They have a more valuable market the less privacy here is." Would you agree?**

No, I don't agree. I do sincerely believe that Facebook could make oodles of money if they worked harder on security and privacy. It may be *harder* work in the short term, but I think it would show long term rewards. Would Facebook do it? I'm not so sure.

Facebook's recently clumsy introduction of a feature which would allow rogue application developers to access users' mobile phone numbers and home addresses (and its subsequent temporary withdrawal while it rethinks its approach) makes me question whether privacy and security are part of the company's DNA.

I see two possibilities: Either Facebook simply doesn't "get" security and privacy, or it just doesn't care. I really hope it's the former. Because if it is, there's still a chance that Facebook can build a network that is secure for its users and will make its users' privacy a top priority.

There's a real problem, though, if Facebook just doesn't care that much about privacy and security. Because 500+ million users are going to and it's very difficult to wrench themselves away from the world's most popular social network.

There's no doubt that there's lots of fun things you can do on Facebook, and that it provides some valuable services. But you must be careful and sensible about how you behave when you're online.

# Are Hackers Finding a Way Into Your Network?

## GFI LANguard

### Award-winning vulnerability management software

To lower the security risk you need GFI LANguard, a solution that provides network vulnerability scanning, patch management and auditing in one integrated package. This award-winning solution allows you to scan, detect, assess and rectify vulnerabilities on your network faster and more effectively.

GFI

WEB & MAIL SECURITY
ARCHIVING & FAX
NETWORKING & SECURITY

*Download your FREE trial version from* **www.gfi.com/lannetscan/**

**tel: +1 (888) 243-4329 | fax: +1 (919) 379-3402 | email: ussales@gfi.com | url: www.gfi.com/lannetscan/**


**Hackers target banks and their customers because - as William Sutton, a notorious 20th century bank robber, is supposed to have said - "that's where the money is". However, following a twenty-first century paradigm, hackers don't burst fully armed into banks but install software known as financial Trojans on their victims' computers.**

These Trojans are ever more sophisticated and show every sign of becoming increasingly so in the coming years as the rewards are large. In this article we will investigate the ZeuS Trojan which according to an FBI estimation has netted around US$70 million for the gang involved.

Financial Trojans of one sort or another have been around for a while. A few years ago a worm called Clampi spread itself by hacking the Windows Administrator account, and then used the rights gained to infect all the other systems on the network.

The problem was that such activity drew attention and as a result intrusion detection systems were able to identify the infected systems. Present day malware is far more discrete, doing all it can to maintain invisibility. This article will look at two such Trojans:

1. ZeuS, chosen because it has proved to be a very resistant strain since it's inception, and

2. URLZone, chosen due to its deployment of "Man-in-the-Browser" techniques.

**ZeuS**

ZeuS has been around since 2007, with the highest level of infection recorded in 2009. In late 2010, its writer, known as Slavik/Monstr, claimed he was 'retiring' and that he was going to hand over the source code of this Trojan to Gribodemon/Harderman - the writer of another financial Trojan called SpyEye.

Recently evidence popped up that the merging of the two codes has produced new malware (tinyurl.com/6knp3el).

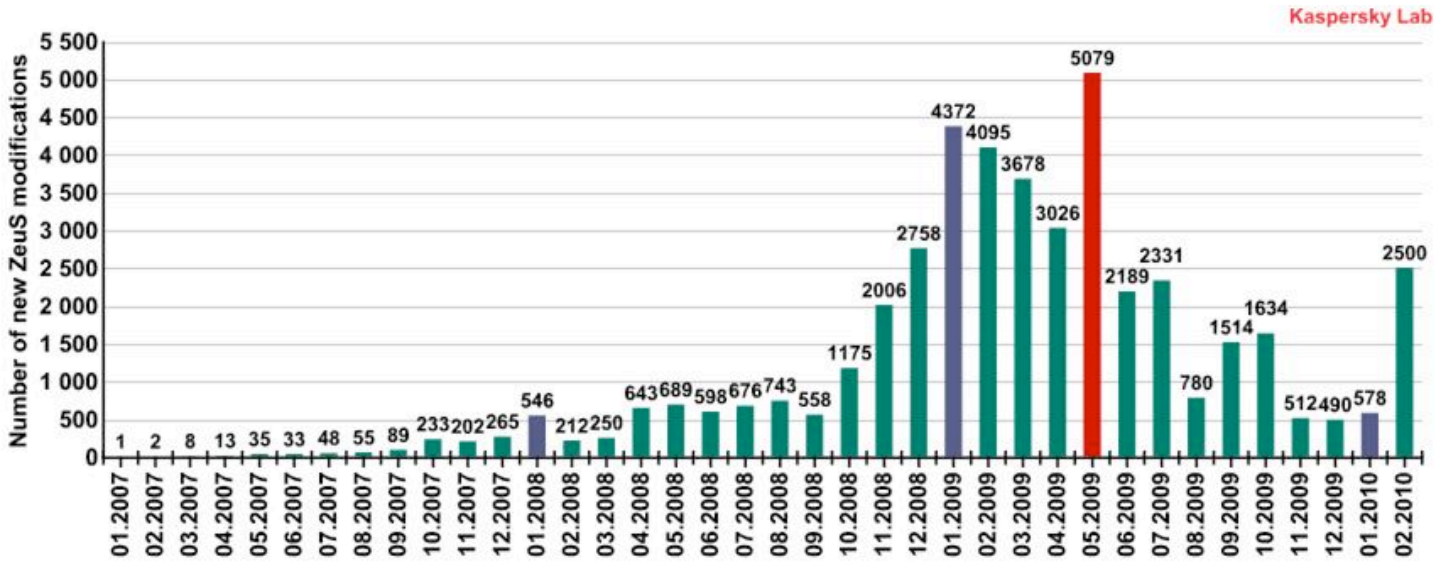



Figure 1. Number of new ZeuS variants (Source: securelist.com).

ZeuS is easily available and offered on sale on many online forums, and its price goes from around US$500 for an older version, to over US$4,000 for the latest one. There are also free versions available but these frequently include Trojan horses themselves that allow the provider to infect the 'purchaser'.

In more recent versions, the ZeuS' developer has made some considerable effort to ensure that versions of his software can only be run only on one machine, making the code hardware aware and requiring a key from the writer to enable the software. By doing this, the writer can increase the income he makes by selling the software to those not able or willing to write their own. Many who do buy the software will try out the scam but fail to make it pay and go out of business. Despite this, a large number of botnets does survive and tempts imitators. This is all good news to the malware writers as they have a ready market of potential bot herders.

Zeus Tracker (zeustracker.abuse.ch) has identified the following number of servers and websites connected with ZeuS on January 22, 2011:

1. ZeuS C&C servers tracked: 543
2. ZeuS C&C servers online: 229
3. ZeuS C&C servers with files online: 40
4. ZeuS FakeURLs tracked: 74
5. ZeuS FakeURLs online: 29

The primary purpose of ZeuS is to steal FTP, e-mail, online banking, and other online credentials/passwords. Figure 2 shows the most targeted websites, highlighting the focus, scope and flexibility of this malware.

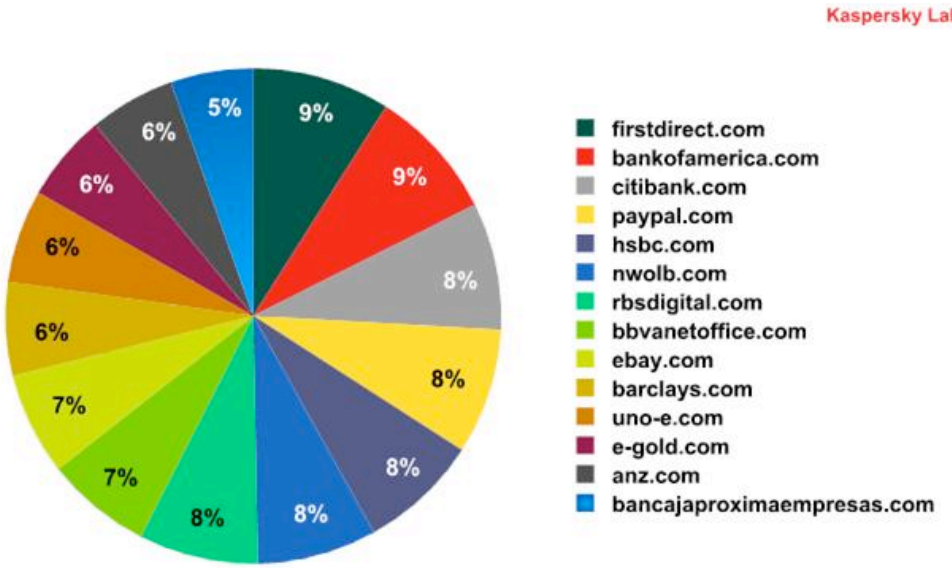



Figure 2. Most prevalent .com domains targeted (Source: securelist.com).

Before it can be deployed, a ZeuS Trojan needs to be built. And this is where the toolkit comes into the equation.

**The ZeuS toolkit**

The ZeuS toolkit not only provides the required malware for installation on a victim's computer but also the necessary web server software for the command and control (C&C) of any botnet that might be generated.

The building of the bot is a three-stage affair and the toolkit provides a wizard for the budding script kiddie to follow:

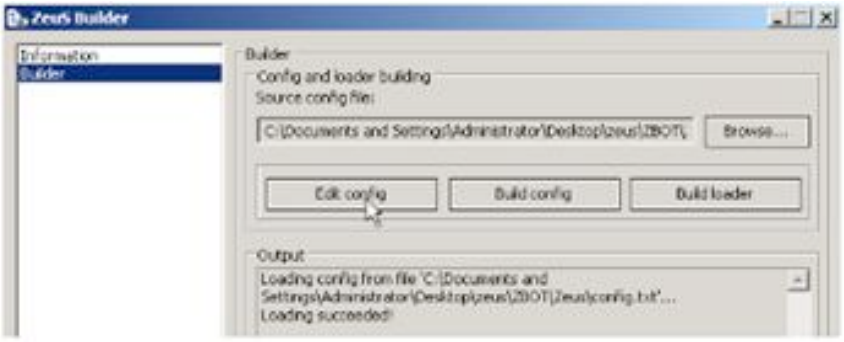



Figure 3. ZeuS Builder interface.

Step one is to configure the bot, a button takes the hacker to the configuration file (see Figure 3). This file then allows the hacker to modify the behavior of the malware, defining where it is controlled, and from to where it injects text and graphics into target websites.

**ZeuS Builder configuration file**

Here are some basic definitions to help you understand this configuration file:

***url_config:*** Location of the server that holds the configuration file, this allows the attackers to define the servers they want to use.

***url_loader:*** Location of the latest ZeuS executable, which allows the Trojan to be updated.

***url_server:*** Location of the command and control (C&C) server, allows the bot herder to control the botnet.

***AdvancedConfigs:*** Location of alternative locations for the configuration file in case the primary location is taken down.

***Webfilters:*** Identifies the URLs to be monitored. The configuration file allows for masks to be created, with wildcards to catch multiple pages.

***WebDataFilters:*** Identifies the URLs to be monitored and specifies the string patterns to be matched. If a match is found, then the data associated with the string patterns is sent to the C&C server.

For example, if a website has a logon, the hacker would look for 'username' and 'password' and when an entry is detected, the text is returned to the C&C server.

Any data sent to the monitored URLs is sent to the C&C server allowing the hacker to access banking credentials and other sensitive information. In fact it is possible to specify a screenshot to be taken at specified moments, say on mouse click when on a certain bank's website.

This enables snapshots of security systems that use virtual keyboards on the screen to enter the PIN number to be taken and feed it back to the bot herder. As the Trojan is effectively positioned above layer 4 (transport layer) of the OSI Model, the data is captured before it is encrypted and much of the security features relied on by banks are thus circumvented.

***WebFakes:*** Redirects the specified URL to a different URL, which will host a potentially fake version of the page.

***TANGrabber:*** The Transaction Authentication Number (TAN) grabber routine allows the hacker to specify the online bank URL that is of interest and to specify the patterns that enables the bot to search for transaction numbers.

***DNSMap:*** Allows the hacker to add entries to the victims HOSTS file and redirect users to sites other than the real one. Another ruse is to prevent access to security sites so that antivirus updates fail.

***file_webinjects:*** The location of a file that contains HTML to inject code into online banking pages.

Many banking sites now deploy strategies that mean the customer is not entering all their data at any one logon. A common example is to ask for just three characters at random from a password. ZeuS helps hackers overcome this by allowing them to inject questions into the web page to obtain the information directly.

As a simple example, “file_webinjects” could define a file that holds the relevant code that will first look for a given input request - like ‘username’ - and then insert an input box underneath it called ‘password’. This would encourage unwary users to enter their entire password, rather than wait for the next screen where the bank only asks for 3 random characters from their password.

Figure 4 shows the form before it has been modified. In this case the word to look for is ‘proceed’, then insert an input box after this line.


Figure 4. Uncorrupted login page.

The example configuration file refers to webinjects.txt as the file holding the required instructions for the text box insertion and if this file contains the following code, the bot looks for the term defined in the ‘data_before’ section and then looks to the ‘data_inject’ section to find the instructions necessary to insert the required input box:

```
set_url http://www.xxx.com/contact.php GP
data_before
name='proceed'*</tr>
data_end
data_inject
<tr><td><input type="password" name="password" id="password" /><td>password></td></tr>
data_end
data_after
data_end
```

Figure 5. Example of webinjects.txt code.

It is even possible to replace HTML by defining the ‘data_after’ section. If this is done, then HTML between ‘data_before’ and ‘data_after’ will be replaced by the HTML defined in ‘data_inject’. From this, it can be seen that it is possible to carry out significant changes to a website. In our simple example, however, after the HTML has been injected, the form now looks like Figure 6.

To the unwary, it will seem natural to enter the password in full and hence the security of the following page is bypassed.

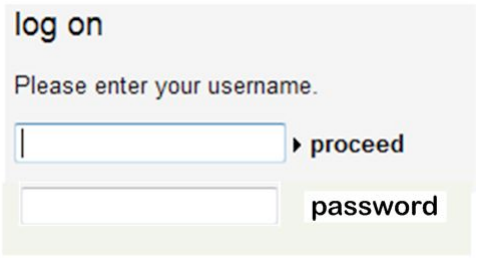



Figure 6. Tainted login page with false password request.

ZeuS comes with a number of built-in commands that make it particularly vicious. These built-in commands are invoked from the C&C server when a bot 'calls home' and the server looks to see if there are any commands for that bot to carry out. The list of commands includes the following:

• Reboot: reboots the computer
• Kos: deletes system files, killing the computer
• Shutdown: shuts down the computer
• Bc_add: initiates back door by back-connecting to a server and allows arbitrary command execution via the command shell
• Bc_del: deletes a back door connection
• Block_url: disables access to a particular URL Unblock_url: restores access to a particular URL
• Block_fake: blocks injection of rogue HTML content into pages that match a defined URL
• Unlock_url: re-enables injection of rogue HTML into pages that match a defined URL
• Rexec: downloads and executes a file
• Lexec: executes a local file
• Lexeci: executes a local file using the interactive user
• Addsf: adds a file mask for local search
• Delsf: removes file mask for local search
• Getfile: uploads a file or folder
• Getcerts: steals digital certificates
• Resetgrab: steals information from the PSTORE (protected storage) and cookies
• Upcfg: updates configuration file
• Rename_bot: renames bot executable
• Getmff: uploads Flash cookies
• Delmff: deletes Flash cookies
• Sethomepage: changes Internet Explorer start page.

The potential bot herder now has a bot, targeting the financial institution(s) of his choosing. Now the hard work begins: the bot needs to be deployed and this is no different than any other malware deployment carried out by e-mail or via websites.

Once a victim is persuaded to activate the malware, what happens next? It depends on how the victim is logged on. When victims are (frequently) logged on as administrators, the malware has an immediate advantage and the following files are installed:

%systemroot%\system32\sdra64.exe
%systemroot%\system32\lowsec
%systemroot%\system32\lowsec\user.ds
%systemroot%\system32\lowsec\user.ds.lll
%systemroot%\system32\lowsec\local.ds

And then it changes the registry entry:

"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" from:
"Userinit" = "C:\WINDOWS\system32\userinit.exe"
To:
"Userinit" = "C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe"

Upon startup, sdra64.exe uses process injection into winlogon.exe to hide its presence. The injected code then starts infecting other processes to carry out the tasks it has been configured to do.
In the case where the victim is running in 'user' mode, the same files are installed but in the following folders:

%appdata%\sdra64.exe
%appdata%\lowsec
%appdata%\lowsec\user.ds
%appdata%\lowsec\user.ds.lll
%appdata%\lowsec\local.ds

And then it changes the registry entry:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"

from: "Userinit" = "C:\Documents and Settings\<user>"
to: "Userinit" = "C:\Documents and Settings\<user>\Application Data\sdra64.exe"

Upon startup, without administrator rights, the sdra64.exe uses process injection into Internet Explorer to hide its presence. Once the malware is installed, it can carry out the tasks for which it was configured: stealing usernames, passwords, security answers, PFX digital certificates and so on. Depending on the configuration, it will then report 'home'. One of the more interesting features is the option to start an IM session (Jabber) which reports the information in near real-time which can allow the hacker use one time passwords before they time-out.

Obviously, they have to be quick, but if they have already managed to obtain the primary authentication details, this feature will provide the remaining part of the puzzle. Later versions of ZeuS improve on the automation by inspecting the C&C database to ascertain if the primary authentication is already known for a particular account, and if it is, it will start an IM session with the hacker so they can use the information immediately.

One final important feature is the ability to deploy VNC and hence to just take over the victim's computer. If there are any hardware devices, embedded cookies or certificates used in the bank's security, this helps the hacker bypass such measures. It also means that the 'attack' on the bank comes from the victim's IP address and adds another level of abstraction when the attack is discovered.

Comprehensive as it is, this attack strategy is still visible. In addition, even though the hacker can receive information near to real time, two-factor authentication is difficult to break requiring the hacker to be very nimble fingered indeed. The breaking of two-factor authentication requires a different approach, such as that implemented by the next Financial Trojan I'm now going to talk about.

**URLZone**

In late 2009, a California-based company called Ferma was reportedly infected with URLZone. The Trojan was subsequently responsible for the theft of US$447,000. Whilst the manager carried out a routine transaction to make legitimate payments, URLZone carried out 27 separate transactions to a number of different bank accounts in the background and subsequently hid these transactions from the manager. This 'man-in-the-browser' (MITB) development is the reason why this Trojan is worthy of study.

There are a number of features that make URLZone so dangerous. Firstly, it tries to take as much of the human element out of the equation as it is possible – a direction in development that I expect to be witnessed often in the coming years. Secondly, this Trojan can bypass sophisticated two-factor authentication. Thirdly, with its ability to mislead the user, the victims are unlikely to become aware of the activity on their account until they receive a paper copy of their transactions.

As many banks are currently reducing the use of paper copies, it will be increasingly difficult for a victim infected by sophisticated malware to know the balance of their account without visiting their bank or a cash point machine.

**Command and Control**

As with ZeuS, URLZone has a toolkit that allows criminals to create a configuration file that allows them to target the institutions they are interested in. URLZone also lists the "money mules" (see below) that will be used to launder the funds stolen from victims.

In addition, it provides the management interface that allows the bot herders to see what is being reported back from any of the systems that have been infected. In fact, this is very similar to the ZeuS toolkit described above. A quick word about "money mules", since they are vital to the success of the scam.

These are usually ordinary people who want to work from home or are unemployed. They see an opportunity to earn money from an apparently reputable company via job adverts that mention 'Payment Processing Agents' or 'Financial Managers'.

These jobs are advertised via e-mail, letters, newspapers, job search websites and other seemingly legitimate arenas.

Once “employed”, they are told that they will receive direct transfers to their bank account and are then told where and how to wire the money.

This is usually done using Western Union since transactions made through these services are irreversible, untraceable and anonymous. For each transfer made, the ‘employee’ gets a commission. In most instances, they quickly find the work drying up as the fraudsters - wanting to spread the risk across a number ‘employees’ and knowing that “employees” are the easiest people for the authorities to find - move on. Furthermore, any money transferred to the “employees” by the Trojan will be recovered by the banks as they are the proceeds of fraud. Hence the “employee” is often left not only unpaid but also left having to pay the money sent to the fraudsters with no way of obtaining recompense.

As with ZeuS and any malware, the plan is to entice unsuspecting users to download and activate the code. The infection process is outside the scope of this article but follows the usual route of infected e-mails and websites. Once downloaded and activated, it copies itself to the root directory:

C:\uninstall02.exe

It then reports its ID back to the C&C servers so that it can be identified in the dashboard. The C&C server downloads the latest version of URLZone and it gets copied into the Window’s System32 directory with a random name. Once installed, URLZone then downloads its configuration file. As this installation process does not infect system files, it must add an entry to the register to ensure it is started each time on reboot:

“HK_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userint.exe”

It then sets itself up as a debugger of userinit.exe, which results in it being started when userint.exe is started. Next it needs to run as a service enabling it to call home and look for programs running on the local machine on a regular basis. It does this by hooking into svchost.exe. It can now check regularly to see if any of the following programs are working:

1. myie.exe
2. iexplore.exe
3. firefox.exe
4. mozilla.exe
5. avant.exe
6. maxthon.exe
7. thebat.exe
8. explorer.exe

Once these programs are running, URLZone will start looking for the targets identified in the configuration file and can start collecting the credentials of the victim.

For example, consider a victim wanting to transfer some money from his bank account to a friend’s. For this example, the bank in question is one that URLZone has been configured to target and the customer is infected with URLZone.

**URLZone operation overview**

The process is as follows:

1. URLZone sits waiting for the customer to make this transfer. It looks for HTML data that is sent using the POST method over https - a good indicator that the information is going to be valuable.

2. When the user confirms a transaction, URLZone silently changes the request that is to be sent to the bank. It records the amount the customer intended to send and who it was to be sent to. Then it changes the recipient account to one belonging to the money mules and defined in its configuration file and changes the amount to be sent. This last value can be very carefully tailored by settings in the configuration file to ensure the account does not go overdrawn, that amounts are random and that they lie within specified boundaries.

3. The bank software will see this request as genuinely coming from the customer and will make the transfer and return the confirmation.

4. URLZone intercepts this return message replacing the recipient of the transfer and the amount transferred to that which the customer

is expecting to see.

The end result is that the victim enters all the authentication information before URLZone needs to start work. The victim sees the transaction go through successfully and sees the right amount displayed on their screen when the transaction is confirmed and remains woefully unaware of the real transaction that has taken place.

This gives the money mules time to transfer the money to the hackers who remain suitably removed from the crime. It also totally automates the crime and the hacker can leave the Trojan to make the required transactions without connecting to the victim's system.

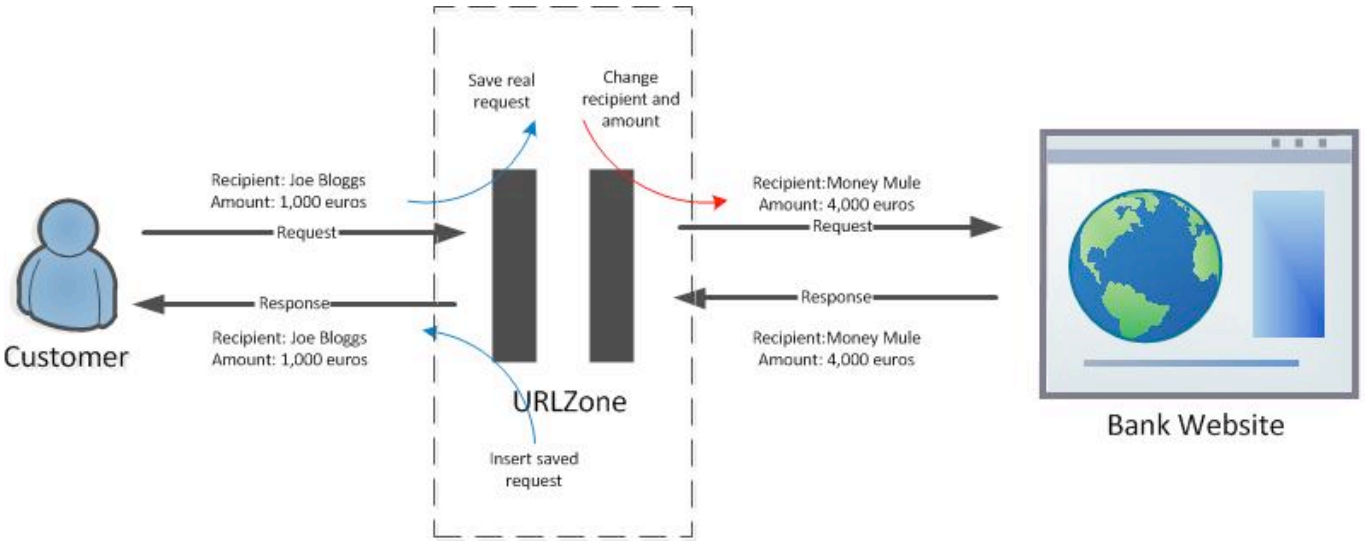



Figure 8. URLZone operation overview.

**Conclusion**

Malware is becoming increasingly sophisticated. The growing availability of development kits - which not only make it easier to build individual Trojans but can also provide the C&C capabilities necessary for managing botnets - compound the problem. Interestingly enough, the original writers are obviously aware that illegal copies of the code are being made and - in an effort to increase their return on their investment - have deployed software that is hardware dependent.

Perhaps the two biggest concerns here are the ability of the current malware to bypass sophisticated two-factor authentication and its ability to automate and hide the transaction from the victim.

Many experts now believe the best way to carry out sensitive transactions over the Internet is to use a dedicated machine. This machine would most likely run Linux and a browser and would be used for nothing else, not for sending e-mails or playing games, not even for everyday browsing! Its sole job should be to access websites the user deems sensitive. This may be a fairly draconian measure but, with many people having older laptops available and Linux being free, this could be a practical solution.

The provision of out-of-band confirmation messages of banking transactions would be beneficial. An obvious choice would be the use of SMS text messages if these are provided by the customer's bank. This would not prevent the crime but would at least enable a user to immediately see that a transaction had been intercepted, cutting down the time needed to detect the fraud.

Security precautions have to be implemented in order to combat this threat. A combination of faster malware-detection techniques and a greater awareness by the end users should make it possible for them to avoid becoming a victim.

Simon Heron is the CTO of Redscan (www.redscan.com), a modular managed security solution provider whose solutions are tailored to suit individual company requirements, and can be delivered either on premises or in the cloud.

# Mobile encryption: The new frontier

by Michael Ginsberg

**As mobile usage for business communications increases, so does the need to protect e-mail and other content through encryption. Despite the fact the encryption technology has been in existence for many years, applying it to e-mail and other forms of communications on the mobile front is a relatively new way of using it and has yet to reach any significant adoption levels.**

However, the rapid evolution of smartphones in the past two to three years has placed the need for mobile encryption at the forefront. The challenges will only escalate as adoption continues. RBC Capital Markets forecasts that by 2012, 35.1% of global handsets or 504 million units (395 million prior) will be smartphones due to the expected shift to e-mail, browsing, applications and content.

Historically, encryption technology has not lent itself to the mobile space. The variety of platforms, the complexity of issuing and managing digital certificates, and the difficulties encountered when decrypting received e-mails/attachments or other types of messaging have made it challenging for organizations to implement encryption policies beyond the PC. In many cases, the rules simply can't be enforced once e-mails make their way to mobile devices; or conversely, encrypted e-mails sent to a mobile device simply can't be accessed without a lot of inconvenience.

The key to enabling encryption on mobile devices is having the infrastructure and workflow to support it. This means adopting a "gateway" and a secure cloud approach that enables encryption rules to be applied automatically to both incoming and outgoing communications under a central management model.

Applying the business rules at the source removes the burden of mobile users having to wait to return to their desktop or place a call to the sender to read an important e-mail. Rather, they can send and receive encrypted

messages on their devices easily and securely from any device and location.

Let's look at the risks associated with smartphone business usage, the importance of encryption in managing that risk, and the best approach for mitigating the risk and maintaining control over corporate data.

**Rising risk**

In the mobile world, risk is rising on two different fronts. The first is the virtually unmonitored use of smartphones for business correspondence and other sensitive communications. Whereas before voice and personal communication were the dominant areas of use, this is rapidly being replaced as business users turn to text, e-mail and file forwarding to manage what used to be desktop functions. While security around these processes is well in hand at the desktop level, security surrounding mobile communications has simply not kept pace.

Hand-in-hand with this increased usage and functionality is a huge uptake in technology that is available to intercept mobile messaging in all forms.

There is a plethora of off-the-shelf, publicly available, free software and firmware resources for the hacking community; as well as a thriving and highly profitable market devoted to the exchange of personal information, credit card numbers, or any other transmitted/stored information that can be stolen in a blink of an eye.

Add to that the vast number of publicly available, unsecured wireless networks, and we can see that the world has made it easy for any tech-savvy person to intercept emails or text messages.

Adding to the security challenge is the consumerization of IT inside enterprises. Today's workers are bringing in a wide range of devices for conducting their day-to-day business communications needs – from iPads and iPhones to Androids and BlackBerries.

This is undermining the traditional centralized IT management approach, because there really isn't a lot an IT manager who is used to controlling a wired environment can do about a stolen iPad that contains confidential information.

## UNWIRED DEVICES TRANSLATE INTO LESS CONTROL AND INCREASED RISK

Simply put, unwired devices translate into less control and increased risk. Even if IT can find a way to control a device at the point of origin, it can't police the unprotected wi-fi network that person might be using during their travels, or the devices and/or users that the information is sent to.

Even if information is sent over a protected network, what network it ends up on at the recipient's end is anyone's guess.

The mayhem became especially prevalent once the iPhone and Android made their way into business users' hands.

In fact, over the last four quarters, growth numbers for the Android platform have outstripped the iPhone, which represents a huge opportunity – or a huge threat – depending on what side of the fence you're on. This is especially problematic given the fact that Android applications can be downloaded from any location, rather than a centrally managed application store.

At the same time, we have yet to see the impact of the Windows phone on the entire equation. It's safe to say at this juncture that every phone is potentially a business device and therefore a danger to security.

**Find the source**

Approaching the mobile security issue with a device lockdown approach is a futile task. When the BlackBerry Enterprise Server was the predominant business platform of choice, and data was centrally provisioned, it was a relatively simple issue. However, with the multiplicity of devices, operating systems, networks, security measures, etc. being used

today, the situation has become unmanageable - if not impossible. End users who constantly want more access to information and applications, and IT managers who are simply trying to impose limits to protect sensitive data, are now deadlocked in an ongoing tug-of-war that seems to be going nowhere.

Granted there are some measures being used, such as remote "wiping" of content from lost or stolen devices, disabling services, or encryption tools that require complex authentication procedures, but these are only addressing a small portion of the overall threat. With hundreds of thousands of permutations of devices out there – and more to come – an entirely new perspective is needed for mobile security.

The key to resolving this escalating need is in fact based on a relatively simple principle: moving applications and data to the cloud, securing it at source, and allowing mobile devices to access it. If done properly, this approach provides a simple, secure platform where data can be centralized and protected.

The philosophy behind this approach is an extension of the "lock and key" approach that has been in force for years.

Basically, data resides in a place where unauthorized users can't reach it; it is kept off the devices used to access it; and with the proper encryption technologies/processes in place, ensures that it can't read if the transmission is intercepted.

## REALISTICALLY SPEAKING, DATA ENCRYPTION FOR MOBILE DEVICES IS STILL IN ITS EARLY STAGES

Realistically speaking, data encryption for mobile devices is still in its early stages. However, conversations with developers around the world indicate that interest in e-mail, voice and other encryption solutions is escalating at a significant rate as smartphone adoption for business has become pandemic.

IT managers are coming to the realization that focusing on ever-changing mobile interfaces carries with it an inherent risk. Subsequently, they are also recognizing that a central server/cloud approach – where encryption policies can be automatically enforced, and users can pick up, login and decrypt messages – is a means to manage the complexities of it all.

Once that information is read, it can then go back to its encrypted state until it is needed again.

Cloud-based encryption of all forms of business communications also enables auditing and reporting, so managers can know when messages have been sent, when and where they have been read and by whom. At this point, e-mail encryption has been among the first applications to utilize this model. This is in large part because it represents one of the largest threats to corporate security.

According to Forrester Research, next to portable storage, e-mail is the second most prevalent area for data leakage. E-mail encryption will shortly be augmented by encryption solutions for voice, SMS and instant messaging – all of which can transcend the issue of which mobile platform is being used.

The rapid escalation of smartphone platforms for business use has created a challenging situation for IT managers over the past few months. With the availability of secure cloud-based services, a centralized approach to mobile security management however is possible, with the right processes and resources in place.

The only thing that is needed now is a concerted effort on the part of business to establish control over an increasingly complex and threatening situation.

Michael Ginsberg is the CEO of Echoworx Corporation (www.echoworx.com), a provider of managed encryption services for complete enterprise email and data protection.


# information security

## foresight in a complex environment

**Master complexity and gain the foresight you need to safeguard your business at Infosecurity Europe 2011**

- Demonstrate clear thought leadership to ensure security is high on the corporate agenda
- Achieve visibility of your mobile workers, cloud providers and web of third party suppliers
- Clearly navigate and understand increasingly complex legislation
- Deliver security to drive and enable clear business growth

**Register FREE* to visit at www.infosec.co.uk**

Follow us on Twitter @infosecurity

Join the Infosecurity Professionals Group

Join the Infosecurity Europe Facebook Group

**Europe's NO.1 Information Security Event**

**19-21 April 2011**

**Earls Court**

**London UK**

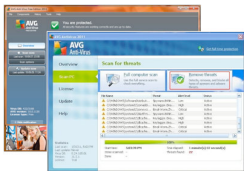
Organised by:

Reed Exhibitions®

infosecurity® EUROPE

*Visitor registration is free online before Friday 15th April. Onsite visitor registration £20


## Rogueware starts misusing names of legitimate AV

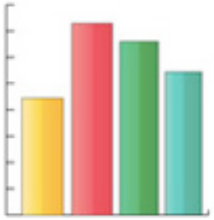


As time passes and users become more and more adept at finding out whether the name belongs to a real or fake AV solution, rogueware developers will have to resort to the more risky business of using names of legal software - and some have started already.
(www.net-security.org/malware_news.php?id=1612)

## Expanding phishing vector: Classified ads

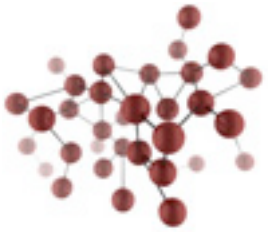
The online classified advertisement services sector has been increasingly exploited as a phishing attack vector by ecrime gangs, a trend confirmed by the growth of attacks abusing classified companies in the first half of 2010, accounting for 6.6 percent of phishing attacks in Q2 2010 alone, according to the APWG.
(www.net-security.org/malware_news.php?id=1613)

## Serious jump in new vulnerabilities exploitation



On a typical month, exploit activity falls between 30 and 40%. Half of new vulnerabilities rated as critical were targeted in January, opening doorways for an attacker to execute any command(s) on a target machine. "It is no secret that software vulnerabilities continue to be disclosed in large numbers on an ongoing basis - especially critically rated ones," said Derek Manky, senior security strategist at Fortinet's FortiGuard Labs.
(www.net-security.org/malware_news.php?id=1615)

## 500,000 stolen e-mail credentials for Waledac's comeback



Almost a year ago, the Waledac botnet was crippled by a legal action initiated by Microsoft which resulted in the takedown of 273 Internet domains that were being used as C&C centers for the infected computers. Security researchers are still monitoring its activities and recently the team from Lastline has managed a peek into a stash of stolen credentials the botmasters have managed to acquire. They found 489,528 credentials for POP3 e-mail accounts and 123,920 login credentials to FTP servers.
(www.net-security.org/malware_news.php?id=1616)

## Zeus evolution: Geographical attack locations

Ongoing research confirms the evolution of Zeus, with a growing number of Web sites that host Zeus variants, as well as the rising volume of networks hosting Command & Control servers for the Zeus botnet swarms. Over the last four months Trusteer's research teams have been analyzing the geographical IP distribution of sites hosting Zeus configurations.
(www.net-security.org/malware_news.php?id=1617)

## Targeted attacks on Abobe Reader files rise

GFI Software revealed continuing high levels of rogue security products circulating during January, and a surge in malware that takes aim at vulnerabilities within Adobe Reader and the PDF file format – two of the top 10 detections are aimed at exploiting holes within Adobe.
(www.net-security.org/malware_news.php?id=1619)

## Zeus Trojan targets UK government

During his speech at the Munich Security Conference, UK's foreign secretary William Hague revealed that the UK government has been targeted with a e-mail campaign containing the well-known information-stealing Zeus Trojan. The campaign started in December, and took the form of e-mails purportedly coming from the White House which contained a link that would take the victims to a page where a variant of the malware would be downloaded.
(www.net-security.org/malware_news.php?id=1621)

## Malware increases by 46% in only one year

There is a steady growth of threats to mobile platforms, according to a new McAfee report. The number of pieces of new mobile malware in 2010 increased by 46 percent compared with 2009. The report also uncovered 20 million new pieces of malware in 2010, equating to nearly 55,000 new malware threats every day.
(www.net-security.org/malware_news.php?id=1622)

## 1 in 3 EU Internet users infected by malware

The EU has a high Internet penetration rate and over two-thirds of the population uses Internet. However, as is the case with other regions, Internet security has assumed significance due to rising incidents of cybercrime. Recently, Eurostat released figures on Internet security in the EU region. The report summarizes the results of a survey conducted to study usage of ICT in 27 member states of the Union.
(www.net-security.org/malware_news.php?id=1624)

## Unregulated mobile app markets are a godsend to malware developers

It's basic economics - as the number of smartphones continues to rise worldwide, so will the number of threats targeting the users of these devices. One of the biggest threats is expected to be malware disguised as or bungled with legitimate applications. The fact that regulated and an even greater number of unregulated app markets are currently springing up left and right, we'll probably not have to wait long for the fulfillment of that particular prediction.
(www.net-security.org/malware_news.php?id=1626)

## Credit score checking app triggers Trojan download

The main reason people get scammed and/or their computer infected online is because they can't contain their curiosity, and that is precisely the thing on which the peddlers of a small application for checking credit scores and criminals records of Brazilian citizens count on.
(www.net-security.org/malware_news.php?id=1628)

## Two BBC sites serving malware via injected iFrame

The visitor doesn't have to do anything except land on the website to become a victim of a so-called drive-by download attack, since the websites have been injected with an iFrame that automatically loads the malicious code from a website parked on a co.cc domain.
(www.net-security.org/malware_news.php?id=1631)

## New backdoor Mac OS X Trojan surfaces

There are many good reasons to choose a Mac machine, and among those is surely the fact that malware for OS X still pops up rarely. Even what seems to be a beta version of a Mac OS X Trojan is enough to raise our heads from the keyboard and take notice, so Sophos' researchers warn about a backdoor Trojan that will quite likely have the ability to take over the infected system and perform a series of unwanted actions.
(www.net-security.org/malware_news.php?id=1643)

## Company wants to bundle spying app in legitimate Android game

How can one deliver spyware to a large number of unsuspecting users? The right answer to that question is - unfortunately - not a unique one, but among the methods is one tried by a company that attempted to convince the developers of a popular Android game to bundle it up with their offering.
(www.net-security.org/malware_news.php?id=1632)

## New type of financial malware hijacks online banking sessions

A new type of financial malware has the ability to hijack customers' online banking sessions in real time using their session ID tokens. OddJob, which is the name Trusteer gave to this Trojan, keeps sessions open after customers think they have "logged off", enabling criminals to extract money and commit fraud unnoticed.
(www.net-security.org/malware_news.php?id=1636)

## Spyware compromises 150,000+ Symbian devices

A new variant of spyware "Spy.Felxispy" on Symbian devices causing privacy leakage has recently been captured by the National Computer Virus Emergency Response Centre of China. Once installed, the spyware will turn on the Conference Call feature of the device without users' awareness. When users are making phone calls, the spyware automatically adds itself to the call to monitor the conversation.
(www.net-security.org/malware_news.php?id=1640)

## Malware-driven pervasive memory scraping

Reports are coming in of a new trend in hacking techniques. Known as 'pervasive memory scraping,' the technique relies on the fact that certain areas of Windows memory are only occasionally overwritten, meaning that data from software that has been closed down on the PC, can still remain for some time after.
(www.net-security.org/malware_news.php?id=1641)

## Banking MitB Trojan effective with most browsers

Man-in-the-Browser attacks are becoming ever more popular with cybercriminals that seek to plunder bank accounts. The latest in a long string of banking Trojans that aids them to do just that is the Tatanga Trojan. Like SpyEye, it can perform automatic transactions, retrieving the mules from a server and spoofing the real balance and banking operations of the users," say S21sec researchers.
(www.net-security.org/malware_news.php?id=1644)


**The 20th edition of RSA Conference, took place in February in San Francisco. Attendees were able to learn about hot IT security's topics through interactions with peers, luminaries and emerging and established companies. What follows are some of the many products and news presented at the show.**

## IronBee: Creating an open source web application firewall

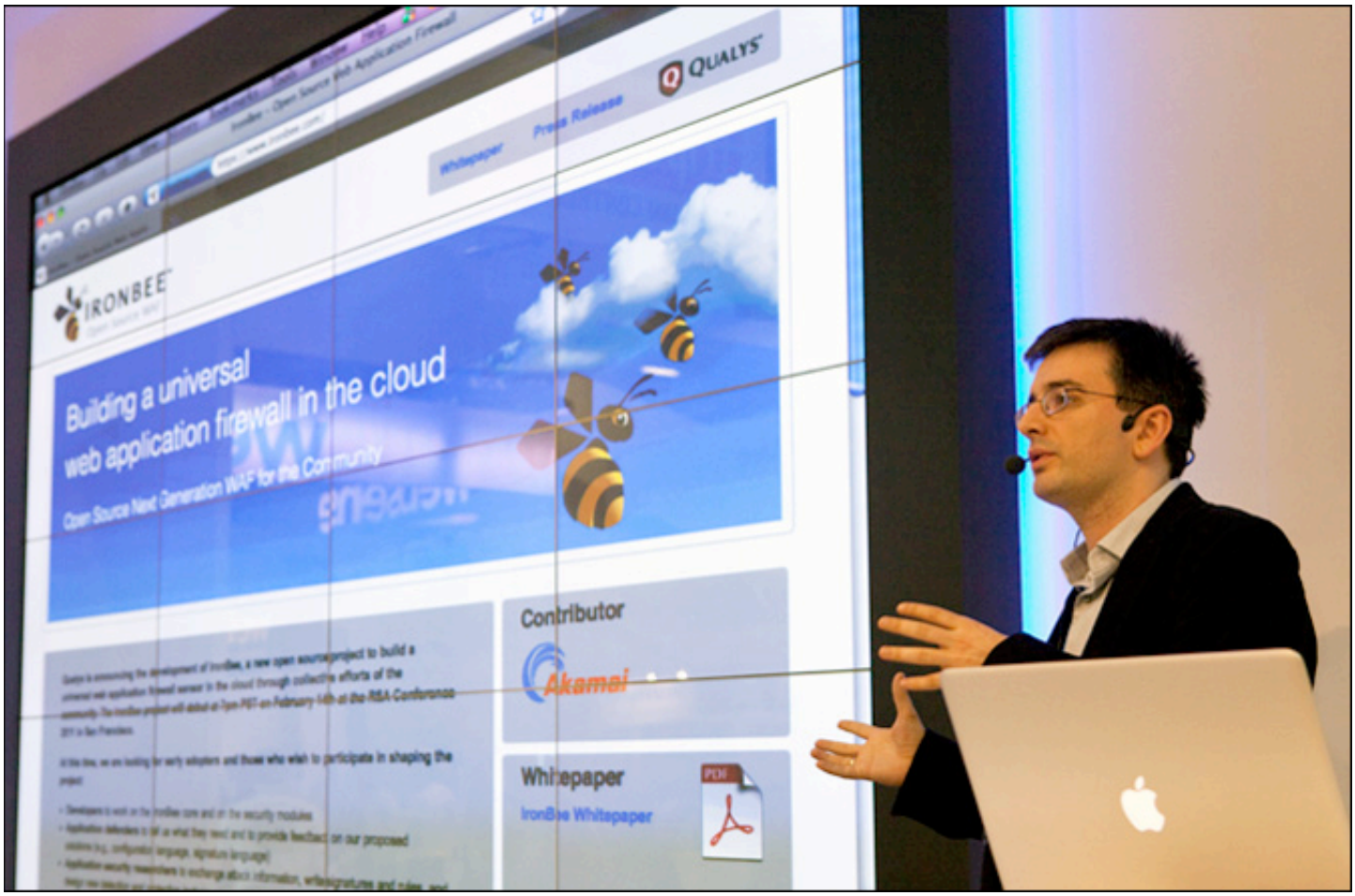
Qualys announced IronBee, a new open source project to provide the next-generation of web application firewall technology. Led by the team who built ModSecurity, the new project aims to produce a web application firewall sensor that is secure, high-performing, portable, and freely available – even for commercial use. (www.net-security.org/secworld.php?id=10589)

## 124 new advanced evasion techniques discovered

Stonesoft discovered 124 new advanced evasion techniques (AETs). Samples of these AETs have been delivered to the Computer Emergency Response Team, who will continue to coordinate a global vulnerability coordination effort. (www.net-security.org/secworld.php?id=10588)

## Licensing platform on a USB stick


INSIDE Secure and PACE Anti-Piracy collaborated to bring to market a portable, convenient, simple to use and robust security device to protect and manage multiple software licenses. (www.net-security.org/secworld.php?id=10593)




Ivan Ristic, the director of engineering at Qualys, during his IronBee presentation.

## Malware and virtual patching info added to QualysGuard

QualysGuard Vulnerability Management now integrates with Trend Micro Threat Intelligence and Trend Micro Deep Security providing customers with live access to the latest information on related malware and available virtual patches, making it easier to accurately prioritize remediation activities and take action to keep data safe. Trend Micro Deep Security (for servers) and Trend Micro OfficeScan Intrusion Defense Firewall (for desktops) provide capabilities to shield host vulnerabilities from attack. Now QualysGuard customers can view information on which vulnerabilities can be mitigated with these virtual patching solutions, including a CVE reference, description of the virtual patch, and a link to apply the patch for immediate protection. (www.net-security.org/secworld.php?id=10585)


## Biometric cabinet lock detects “life in the finger”

Black Box announced it is demonstrating its Intelli-Pass Biometric Access Control for Cabinets. The solution is a complete software-controlled security system and features a fingerprint sensor on the front of the cabinet, allowing access to both the front and rear doors. A key competitive differentiator for the product is its ability to detect “life in the finger.” The Intelli-Pass system detects blood flow, eliminating methods for spoofing fingerprints such as making photocopies or transferring fingerprint imprints to gloves. (www.net-security.org/secworld.php?id=10607)

## An in-depth view of IT policy compliance

Qualys released QualysGuard Policy Compliance 3.0, providing more comprehensive policy compliance scanning capabilities without the need to install agents. Version 3.0 expands support for new operating systems and adds support for scanning databases and network devices – providing customers with a full, in-depth view of IT policy compliance across all assets. (www.net-security.org/secworld.php?id=10595)


## One in 10 IT pros have access to accounts from previous jobs

According to a survey that examines how IT professionals and employees view the use of policies and technologies to manage and protect users’ electronic identities, the sharing of work log-ins and passwords between co-workers is a regular occurrence. The results of the survey underscore how these technologies, or lack thereof, are making it more difficult for employees to get their jobs done. (www.net-security.org/secworld.php?id=10620)


## Web application scanning on a new level

Qualys released QualysGuard WAS 2.0 with several major enhancements to help customers catalog their web applications on a global scale and scan them for vulnerabilities that can lead to exploitation. The new release, delivered via the QualysGuard SaaS platform and its new Java-based backend comes with a new Web 2.0 User Interface that raises the bar in terms of ease-of-use, flexible reporting and automation of scanning tasks. (www.net-security.org/secworld.php?id=10590)

## Information security pros stretched thin and overworked

A study based on a survey of 10,000 information security professionals worldwide finds that a growing number of technologies being widely adopted by businesses are challenging information security executives and their staffs, potentially endangering the security of government agencies, corporations and consumers worldwide over the next several years. (www.net-security.org/secworld.php?id=10630)

## Cloud-based software reputation platform


Bit9 announced an open, cloud-based reputation platform available to assess the trustworthiness of software. The Bit9 GSR is now accessible via an open API allowing the global cyber security community to easily integrate their solutions with the Bit9 GSR Platform. (www.net-security.org/secworld.php?id=10618)

## Next generation Security-as-a-Service platform

Qualys introduced its Security-as-a-Service platform to host the QualysGuard IT security and compliance SaaS suite of applications in the cloud. The platform provides an integrated framework with new functionality in all Qualys security and compliance applications. (www.net-security.org/secworld.php?id=10615)

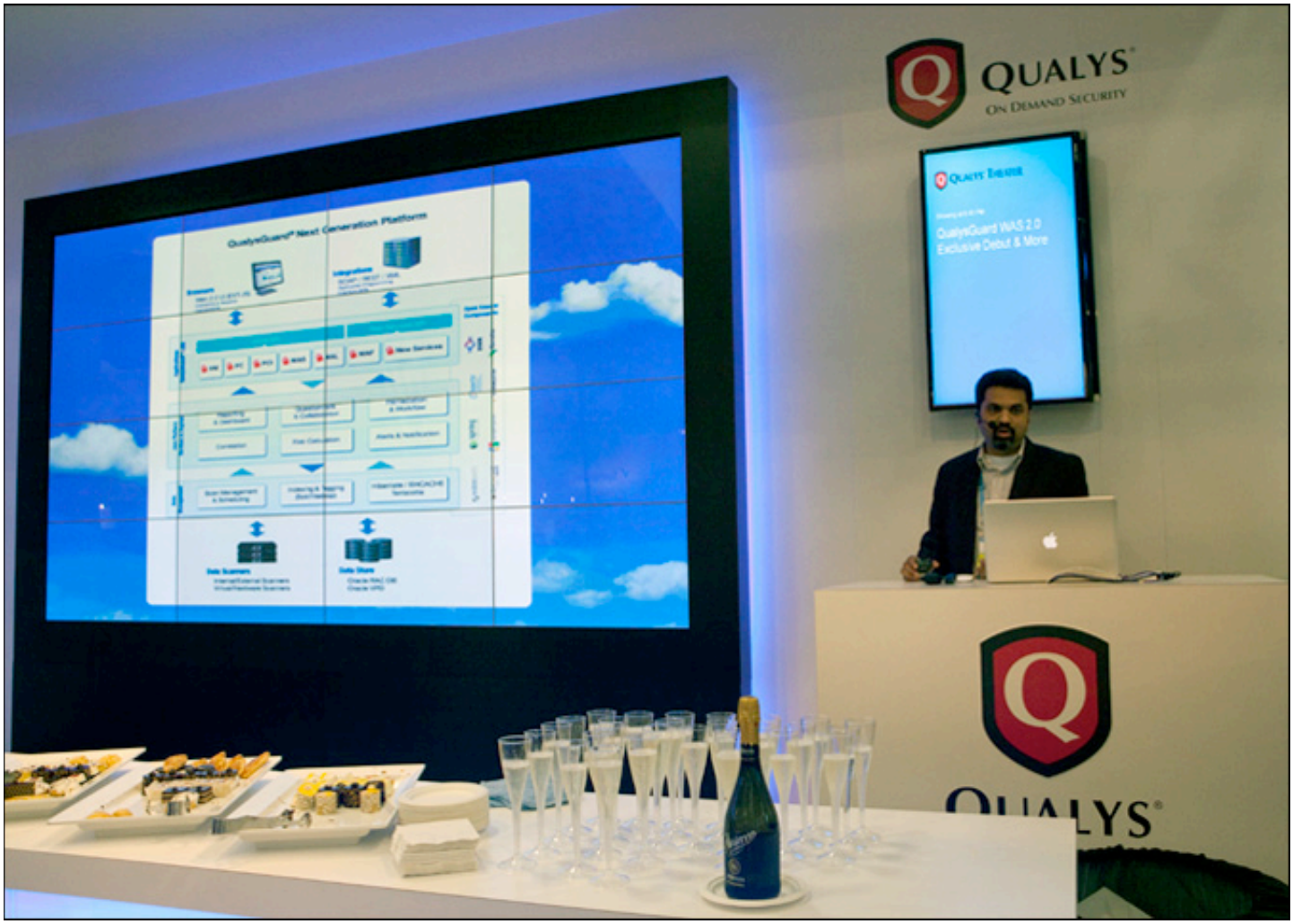
## Distributed security architecture for security enforcement

Cisco is introducing a new highly distributed security architecture that manages enforcement elements like firewalls, Web proxies and intrusion-prevention sensors with a higher-level policy language that is context-aware to accommodate business needs. These next-generation scanning elements are independent of the physical infrastructure and can be deployed as appliances, modules and cloud services. (www.net-security.org/secworld.php?id=10628)


Mike Shema, Senior Security Engineer at Qualys, talking about the QualysGuard Enterprise Suite.

## Real-time threat intelligence delivery

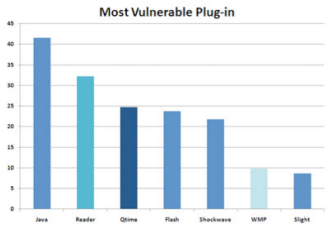

As the threat landscape is evolving on a daily basis, it is imperative that organizations and their IT security teams are aware of the latest vulnerability threats. Perimeter E-Security's Threat Intelligence Service, powered by Secunia, delivers the latest vulnerability information to customers. The service delivers only what is relevant to each customer, reducing the time for planning and remediation that may be required. (www.net-security.org/secworld.php?id=10626)




Sumedh Thakar, the VP of Engineering for Qualys showcasing new products.

## Real-time threat intelligence delivery

Wondering how secure your browser is? Qualys CTO Wolfgang Kandek presented their research which clearly shows that browser security is alarmingly bad. Data was gathered by Qualys BrowserCheck, a tool that scans your browser looking for potential vulnerabilities and security holes in your browser and its plug-ins. Detailed analysis of the data showed that only about 20% of security vulnerabilities are in the browsers and the great majority of security issues comes from the plug-ins installed in them. (www.net-security.org/secworld.php?id=10617)



# SECURITY AS A SERVICE

## NOW AVAILABLE AT A BROWSER NEAR YOU

Software-as-a-Service (SaaS) has been described as the most disruptive delivery model to ever face the enterprise software market for one simple reason: ***it works***

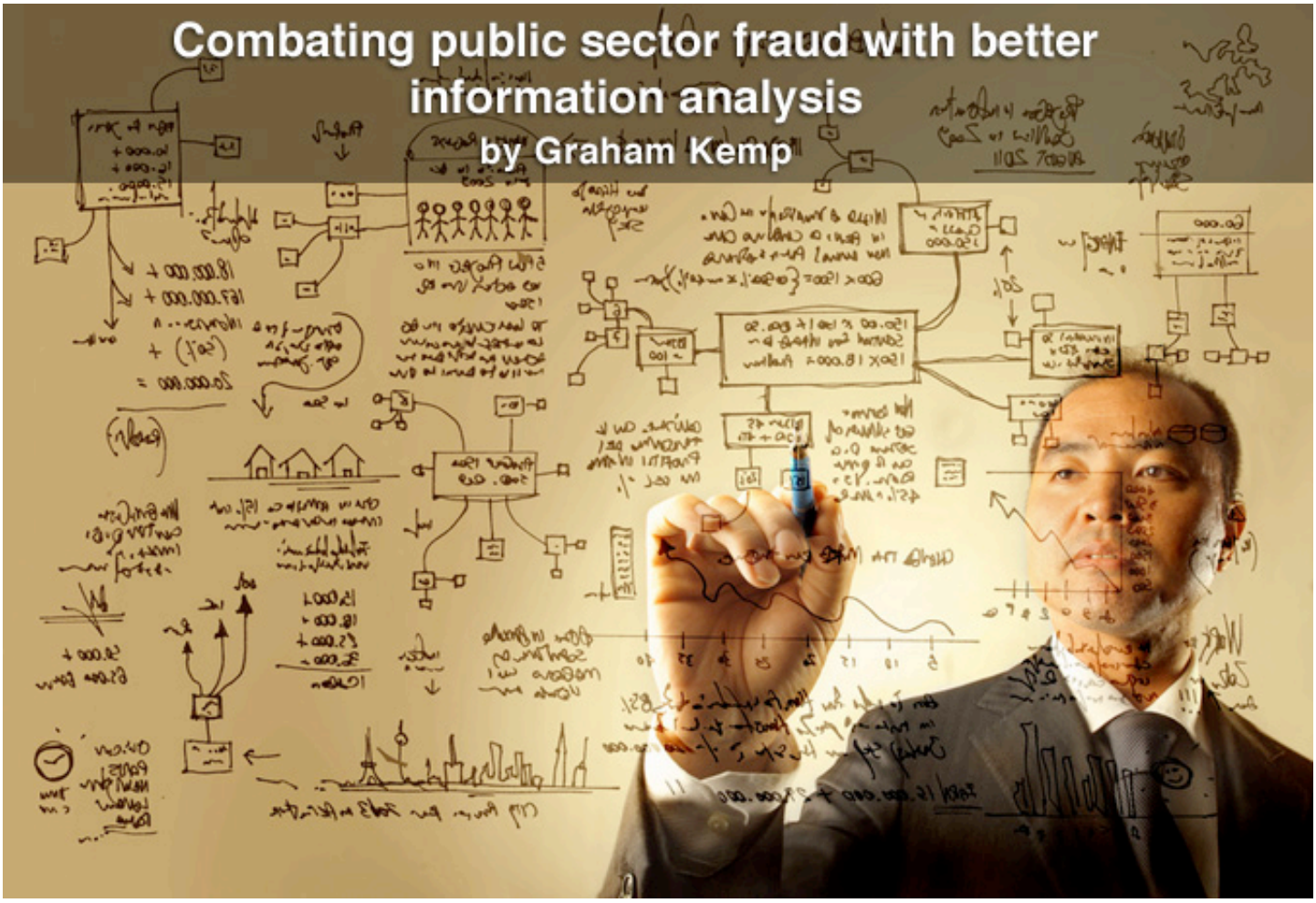
Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard® is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year — with no software to install and maintain.

**For a free trial, go to a browser near you.**

www.qualys.com/SaaSTrial

# Combating public sector fraud with better information analysis

by Graham Kemp



**The latest government initiative to crack down on fraudsters can only be achieved through smarter information analysis.**

Tackling fraud is a major part of the latest government strategy to reduce the billions of pounds lost to fraud and error every year. Since the coalition government came to power, tackling fraud has been elevated from a moral issue with financial implications to being part of the solution to reduce the public sector budget deficit.

At an estimated cost of £30 billion each year, combating fraud within the public sector is an obvious place to start. Every penny lost could be redirected to improving performance and strengthening frontline services.

But central and local government, as well as the National Health Service (NHS), must work together to tackle a plethora of attacks from internal errors and tax avoidance to organized crime.

The National Fraud Authority (NFA) recommends taking cues from the private sector by adopting a new attitude to information management and using advanced analytics to identify problem areas to bolster prevention and detection initiatives. Either way, government can no longer afford to continue spending public resources on investigating fraud retrospectively as it continues to evolve at an alarming pace.

This article explores the many types of public sector fraud and explains how harnessing and exploiting data gathered using analytics can help identify, predict and prevent the high prevalence of fraud and error plaguing the public sector.

## Rising incidence of fraud in the public sector

Referring to the growing deficit as 'the most urgent issue facing Britain', the government has instructed Whitehall departments to come up with plans for savings of up to 40 per cent. Against this backdrop, the NFA revised its estimates on the true cost of fraud, equating it to £30 billion per year, up 39 per cent on previous forecasts.

There are a number of reasons for rising fraud levels including recessionary fall-out, continued cutbacks, and the growth of online services. History proves that difficult economic times see an increase in fraudulent activity including both organized and opportunistic crimes as unemployment rates rise in line with benefits claims. As public sector staff struggle to cope with additional workloads with no resource to hire additional staff, administration errors also increase.

The move towards online channels for delivering public services has also resulted in an exponential growth in the amount of data collected, giving rise to new types of fraud that can not be tackled using traditional methods. As a result the need to deliver 'more for less' can lead to counter-fraud control investments being reduced or neglected, making the public sector an attractive target for fraudsters.

### Fraud is a battle on two fronts

The impact of the recession has meant the incident of identity fraud is also on the rise. Fraud prevention agency Cifas discovered that the incidence of identity fraud rose by 14 per cent in the first six months of 2010, compared with the previous year, as a consequence of the recession. A recent survey by the insurance group RSA revealed that 1.4 million UK adults agree that hard economic times mean committing insurance fraud is more socially acceptable.

But criminals are not the only threat facing the public sector. It is a common misconception that public sector fraud is mostly external. But internal fraud is also a major problem. In fact over a third of civil servants believe that internal fraud is the biggest threat to the appropriate distribution of funds. According to a PricewaterhouseCoopers report, internal fraud accounts for 39% of fraud cases in the UK public sector, with the firm speculating that the number will soar as pay freezes and low morale and stress increase pressure on public sector employees.

This type of fraud ranges from managers manipulating data to meet stringent targets, to procurement fraud, administration errors and even selling sensitive information to third-parties. A separate report by the Audit Commission warns of an increase in recruitment fraud as more candidates give false information or withhold details in a bid to secure limited positions in the sector.

**The move towards online channels for delivering public services has also resulted in an exponential growth in the amount of data collected, giving rise to new types of fraud that can not be tackled using traditional methods.**

Furthermore, fraudsters are now becoming more familiar with the way current detection solutions work and are adapting and evolving their attacks accordingly. They can often stay one step ahead of the system and as a result, the public sector has become a prime target for organized fraud.

Fraudsters understand the siloed nature of government departments so recognize that crimes like identity theft can often easily go undiscovered as inconsistencies across sectors are much harder to identify. With few benefit fraud cases making it into court (in 2009, just £426 million of fraud against the public sector went before the Crown Courts), it is no surprise that the public sector has become a target for fraudsters.

### Dealing with rising fraud levels

Public sector organizations will have to prioritize. Dealing with fraud in its various forms while balancing increased pressure for savings can only be achieved by treating information as an asset. This needs to be collected and analyzed in smarter ways to detect fraud before monies are paid out.

To tackle the rising trend in fraudulent activity, the government needs to invest in predictive, collaborative systems that support data sharing and integration, analytical profiling and stronger identity authentication. Only these will be able to combat the evolving nature of today's sophisticated fraudster.

To truly exploit new technologies and protect the public purse, key cultural changes need to happen.

The growth of online information means the government is increasingly data rich, and working to resolve the current siloed nature will help gather a significant insight into fraud.

The coalition government is looking to support this by implementing a cross-departmental, data-matching and fraud investigation service as part of its new fraud and error strategy, and has already launched a new joint strategy between HM Revenue and Customs and the Department for Work and Pensions.

In addition, private companies contracted to work for the public sector may be asked to open up their data. Treating information as an asset, and sharing it, means public sector organisations can adopt a more proactive approach to predicting fraud, reducing unnecessary investigations and diverting resources to investigate real criminals.

### A hybrid approach

There are four approaches to fraud and error detection. Used alone, none can address all aspects of fraud, minimize unnecessary investigations and prioritize lines of investigation, but used together they can encourage success:

• Rule-based detection systems, traditionally used by the UK public sector, identify potential instances of fraud based on behaviors that have been fraudulent in the past. But, they are ineffective in detecting new kinds of fraud or previously unknown patterns, so become meaningless as strategies become more complex.

• Anomaly detection can detect unknown or unexpected patterns by comparing data like-for-like or within peer groups. Once deviant behavior is identified, rules can be developed to flag up that behavior in the future. However, this method can identify 'fraudulent claims' incorrectly.

• Advanced analytics applies the latest data, text and web mining technologies to identify fraudulent and errant behaviors.

It 'learns' what good and fraudulent behaviors look like so it can uncover rules that would be hard for a human being to identify, as well as providing an indication of the reliability of the rule. Data such as text, video and audio can be analyzed. This is the only way to put preventative action in place.

• Social network analysis, done at the same time, uncovers previously hidden links and makes them visible by aggregating data from multiple sources that share a common piece of information.

This provides a holistic view of fraud. It looks beyond the individual, considering families, neighbors and associated groups of people who could potentially form organized crime networks. When a link is found at a network-wide level, the chances of it being a correct identification of fraud are much higher.

A scalable and flexible approach is the only way to ensure that all types of fraud can be prevented. For the coalition government, it's now time to put an end to the problem and concentrate time and money on leading the country out of austerity.

If Britain is going to take on its most pressing issue, reducing the £155 billion deficit, it must start to value and prioritize its data to make smarter decisions about how to reduce fraud in order to reallocate resources towards strengthening and prioritizing frontline services for deserving citizens.

Graham Kemp is the head of SAS' public sector practice in the UK. In his role, Graham is responsible for helping SAS' public sector customers use information as a strategic asset to accelerating the deficit reduction by optimizing performance and mitigating the risk of failure.


## Scapy

(www.net-security.org/software.php?id=485)

Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer.

## Nmap

(www.net-security.org/software.php?id=1)

Nmap is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

## USB Blocker

(www.netwrix.com/usb_blocker_freeware.html)

The freeware NetWrix USB Blocker enforces centralized access control to prevent unauthorized use of removable media that connects to computer USB ports, for example, memory sticks, removable hard disks, iPods, and more. USB port access control is a very important aspect of your endpoint security, no matter how good your antivirus and firewall are. The USB device lockdown protects your network against malware and prevents theft of sensitive corporate data.

## Network Infrastructure Change Reporter

(www.netwrix.com/network_infrastructure_change_reporter_freeware.html)

Network Infrastructure Change Reporter is a network device auditing and reporting tool that tracks changes to all network devices and their settings. It automatically detects new devices in specified IP ranges and tracks changes to their settings, such as modifications in IP routing tables, firewall rules, security settings, and protocol parameters. With this software, network administrators can automatically document every single change made to managed devices and detect unmanaged and rogue devices.


**Stefan Frei is the Research Analyst Director at Secunia. In this interview he discusses security research, patching issues, vulnerability management challenges, as well as Adobe and Microsoft.**

**Your research shows that even though the number of discovered vulnerabilities has slightly decreased in the last two years, the worrying fact is that 84 percent of all those found in 2010 can be exploited from a remote location, and that 69 percent are tied to third-party products that may or may not have a quality patching mechanism in place.**

**Since this opens a huge door for cybercriminals what advice would you give to those managing large corporate networks with thousands of machines? On the other hand, what can end users do?**

Deployed software, on business and private end-points alike, requires constant attention due to the continued discovery of new vulnerabilities and the release of patches. As our data shows, third-party (non-Microsoft) programs pose a bigger threat than Microsoft programs and the Operating System. Patching and keeping Microsoft programs and the Operating System up-to-date have become routine over the years as these are still perceived as the main threat. Furthermore, this perception and the familiarity with "Microsoft updates" makes patching these programs and the Operating System easy. On the other hand, identifying and patching the remaining third-party programs is still a complex undertaking without suitable tools and processes.

As you can't manage what you can't measure, the first step to secure end-points is getting an accurate inventory of ALL programs installed in ones infrastructure, including ALL third-party programs. This inventory can then be security tracked – matching it against information about new vulnerabilities and the availability of patches ("Vulnerability Intelligence") to determine the threat and act upon it. Like running backups and updating anti-virus signatures, the complexity and frequency of the actions required by this process requires tools and automation - especially in larger infrastructures.

***Step 1:*** Get an accurate inventory of the infrastructure.
***Step 2:*** Identify ALL programs that are end-of-life or programs with missing patches.
***Step 3:*** Prioritize the creation of patch-packages and their roll-out based on the information gained in steps 1-2.
***Step 4:*** Roll-out the patches.
***Step 5:*** Verify that the patches are actually installed.

For enterprises this means coupling existing tools used to distribute software and software updates (e.g. SCCM, WSUS) with a process to prioritize and roll-out patches. Our experience shows that the software inventory in larger infrastructures is rather dynamic and changes frequently - this is aggravated by the fact that many popular third-party programs can be installed by users without requiring administrative privileges. Thus automation and frequent monitoring of the infrastructure is key to handle the task.

Our data shows that 50% of the end-users have more than 66 programs from more than 22 vendors installed. Thus for end-users too, the complexity of this task can not be handled manually. For end-users we therefore recommend running a tool that automatically identifies all insecure programs installed and is capable of patching a growing number of third-party programs, such as the free Secunia Personal Software Inspector (PSI) for example.

## 50% OF THE END-USERS HAVE MORE THAN 66 PROGRAMS FROM MORE THAN 22 VENDORS INSTALLED

**What should mobile users do in order to reduce the time between the moment a patch is released and the moment it's finally patched?**

The challenges associated with a mobile workforce are the following:

A) If applicable, how can mobile end-points connect to the Internet while being off-site?
B) How can you ensure that mobile end-points are protected and receive the required patches while being off-site?
C) How do you handle mobile end-points that are potentially infected when they connect back to the infrastructure (and compromise other internal systems)?

A) and B) There are several ways to minimize the chances of mobile end-points becoming infected while being off-site. E.g. Harden the end-point and disable the networking of the end-point while being off-site. This includes disabling non-network infection vectors such as USB drives and CD-ROM.

If the end-point needs networking access, restricting access to the Internet only though the corporate network by a VPN tunnel. Thereby the end-point enjoys the same perimeter protection (proxies, AV, IDS/IPS) as the on-site clients. Upon connecting to the VPN the required updates can be pushed to the end-point with the existing patch process.

Furthermore, with a terminal service solution the end-point connects remotely to the business applications, which are run, managed, and patched on-site. The mobile end-points only need a minimal set of software to connect via VPN and a terminal service client. This lowers the attack surface and limits the threat should the end-point get infected.

C) When mobile end-points come back and are connected internally, they should first connect to a quarantined network only.

There the required updates (software and AV) can be pushed out and a health check can be completed. Only connect the end-point to the internal network when confirmation has been received that it is not compromised.

**Based on what you've seen in the field, how important is vulnerability management in the overall security architecture? Why do you think some companies still think it's not that important and shift all the blame onto software developers?**

Many organizations do not want to implement vulnerability management as it would expose many vulnerabilities that can no longer be ignored and would require dedicated time and resources. So they prefer to ignore the problem. They further draw comfort from the perception that nothing severe has happened in the past, and therefore their strategy of avoidance has seemingly paid off.

This approach, however, is seriously flawed. Modern malware is programmed to be stealthy upon compromise, and is therefore difficult to detect. Recent research found up to 9% of the end-points in large enterprises bot-infected, despite best-of-breed perimeter protection.

Look at the problem from the attacker's perspective. Cybercriminals do not care about the difficulties end-users and businesses face to keep their infrastructures secure, and they don't care who you apportion blame to. They only care about the most efficient way to compromise systems. Cybercriminals carry out vulnerability management (from the attacker's perspective) to systematically identify the easiest and most robust way to compromise hosts, and then automate the task. Modern malware does not use a single exploit, it comes packaged with dozens of exploits that are automatically tried against the target systems until the first exploit succeeds and infects the host. Thus, one unpatched vulnerability, even in an obscure third-party program, will be exploited when the program is used or exposed.

Effective vulnerability management is therefore a necessary first step for any defender. Again, you can't manage what you can't measure.

Without vulnerability management you have no idea where your weak points are or where and how to best allocate and prioritize your limited resources, while the adversary is well aware where to focus his attack. Thus, vulnerability management is about doing the right thing – what is necessary to best focus your limited resources with respect to security. Whereas in contrast, resources spent on feature updates do not lower your attack surface.

Furthermore, prevention is more effective than remediation. Vulnerability management with an effective patch process is better than thousands of anti-virus signatures as a patch remediates the root cause - and renders any number of polymorphic attack vectors ineffective. Our data shows that 65% of the vulnerabilities affecting a typical end-point had a patch available upon the disclosure of the vulnerability, thus visualizing the effectiveness of vulnerability and patch management. You cannot blame the software vendor for being compromised after a patch was available.

## YOU CAN'T MANAGE WHAT YOU CAN'T MEASURE

**What's your take on the progress Microsoft and Adobe have done in the security arena in the past year? Are they doing enough to mitigate the serious security issues affecting their products? Is a monthly patch cycle enough or should patches releases occur more often?**

It is great to see vendors investing in security and it seems that there is a return on the investments made by Microsoft, however the initiatives made by Adobe are still fairly new and it is a bit too early to clearly conclude whether they are enough.

A monthly release schedule is very convenient for customers and, for the majority of vulnerabilities, a monthly schedule will suffice. However, occasionally vulnerabilities are disclosed and even exploited prior to the release of a patch.

In these cases it is crucial that the vendors make out-of-band releases as rapidly as possible and even bypass some of their usual internal QA processes to ensure that their customers can protect themselves - after all, a patch is the best way to protect against exploitation.

**What kind of vulnerabilities do you expect to dominate the security landscape in the next year or two? What should administrators be on the lookout for?**

We do not expect any significant changes in the near future. Administrators should pay particular attention to their actual inventory. Too many neglect keeping track of all their software and appliances, thus they fail to stay up-to-date with information about vulnerabilities and other guidance regarding how to safely maintain this.

Cybercriminals go after easy prey. From a criminal's perspective: #targets x #vulnerabilities equals opportunity. It is expected that about 2 billion users had Internet access by the end of 2010.

Thus, in no specific order:

End-points are prevalent and a very dynamic, hard to secure, environment.

As large software vendors can invest considerable resources in the security of their products, third-party programs from smaller vendors are a softer target and will therefore continue to be exploited in the near future.

The rise of sophisticated mobile devices with access to the Internet and business networks (phones, tablets) make them an increasingly valuable target for criminals.

We therefore expect more vulnerabilities in such devices.

With the cloud computing approach it becomes even more important to secure end-user PCs because these hold the credentials used to access critical data which are available 24/7 in the cloud, thus a small and brief leak of data from an end-user PC can have long-term implications as the compromise of cloud credentials may go unnoticed for a prolonged period of time.

Embedded devices become more prevalent, powerful, and are also increasingly connected to the Internet.

Despite the fact that embedded devices are computers running complex software, they are not perceived as such and thus easily slip under the security radar (e.g. who has a patching process for their networked printers?). We expect more vulnerabilities in such devices.

MIS TRAINING INSTITUTE'S

# INFOSEC WORLD

## CONFERENCE & EXPO 2011

### Over 70 Timely Sessions Covering All Areas of Information Security

- Social Networking: How to Mitigate Your Organization's Risk
- Managing Mobile Devices
- Controlling Privileged Users (And Everyone Else) in a Distributed World
- Metrics from a Risk-Based Approach
- Hacking and Securing iPhones and iPads
- Hard-Drive Forensics
- Next-Generation Firewalls
- Securing Content in SharePoint
- Strong Authentication – Not Just About Two-Factor Hardware Tokens Anymore
- The Seven Most Creative Failures in Web Application Security
- How Hackers Bypass Windows Protection Mechanisms
- Anatomy of a Database Attack
- Securing the Collaborative Environment in a Web 2.0 World
- Staying Out of Trouble with Wi-Fi Wireless Network Security
- Securing VMware Hosts and the View Environment
- State of SSL on the Internet
- HTML5 Vulnerabilities and Precautions
- And much more...

April 19-21, 2011 • Orlando

Disney's Contemporary Resort

Optional Workshops April 17, 18, 21-23

**CO-LOCATED SUMMITS:**

CISO Executive Summit

Secure Cloud & Virtualization Summit

IT Audit Management Summit

Earn up to 51 CPEs!

### KEYNOTE SPEAKERS

**Roger W. Cressey**
*Counterterrorism Analyst, NBC; Former Presidential Advisor*

**Marcus J. Ranum**
*Chief of Security,* Tenable Security, Inc.

**Bob Sullivan**
*Senior Technology Correspondent,* MSNBC

**Chris Nickerson**
*CEO,* Lares Consulting; featured member of TruTV's *Tiger Team*

FOLLOW US ON twitter twitter.com/infosec_world

www.misti.com/infosecworld

MIS TRAINING INSTITUTE The International Leader in Audit & Information Security Training

PLATINUM SPONSOR ORACLE

VIRTUALIZATION SUMMIT SPONSOR RSA The Security Division of EMC, McAfee

GLOBAL EDUCATION SPONSOR (ISC)²

ASSOCIATION SPONSORS ISSA, WITI, INFRAGARD

PREMIER MEDIA SPONSOR SC MAGAZINE


**A scribbled signature may have been enough to verify your identity 20 years ago, but today's online world requires more advanced — and authenticated or encrypted — methods of proving who, or what, you are online or within a digital environment.**

Enter digital certificates — an authentication method that has an increasingly widespread role in today's online world.

Found in e-mails, mobile devices, machines, websites, advanced travel documents and more, digital certificates are the behind-the-scenes tool that helps keep identities and information safe.

## What are digital certificates?

Developed during the eCommerce boom of the 1990s, digital certificates are electronic files that are used to identify people, devices and resources over networks such as the Internet.

Digital certificates also enable secure, confidential communication between two parties using encryption.

When you travel to another country, your passport provides a way to establish your identity and grant you entry. Digital certificates provide similar identification in the electronic world.

Certificates are issued by a certification authority (CA). Much like the role of the passport office, the responsibility of the CA is to validate the certificate holder's identity and to "sign" the certificate so that it is trusted by relying parties and cannot be tampered with or altered.

Once a CA has signed a certificate, the holders can present their certificate to people, websites and network resources to prove their identity and establish encrypted, confidential communication.

A standard certificate typically includes a variety of information pertaining to its owner and to the CA that issued it, such as:

• The name of the holder and other identification information required to identify the holder, such as the URL of the Web server using the certificate, or an individual's e-mail address
• The holder's public key, which can be used to encrypt sensitive information for the certificate holder or to verify his or hers digital signature
• The name of the certification authority that issued the certificate
• A serial number
• The validity period (or lifetime) of the certificate (i.e., start and end date)
• The length and algorithm of any keys included.

In creating the certificate, the identity information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on packaging — any tampering with the contents is easily detected.

Digital certificates are based on public-key cryptography, which uses a pair of keys for encryption and decryption. With public-key cryptography, keys work in pairs of matched "public" and "private" keys.

In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Since these keys only work as a pair, an operation (e.g., encryption) executed with the public key can only be undone or decrypted with the corresponding private key, and vice versa.

A digital certificate can securely bind your identity, as verified by a trusted third party, with your public key.

## Core to a digital world

At one point, the use of digital certificates was limited to secure sockets layer (SSL) implementations and public key infrastructure (PKI) environments. And while those remain two cornerstones for the technology, their value has been realized and expanded to help secure people, machines, devices and environments alike.

## The SSL start

The use of SSL digital certificates to encrypt transmissions between Web browsers and Web servers remains a monumental development of the eCommerce boom. From Internet shopping to online-banking to Web-based stock trading, SSL certificates were the catalyst for innovation that made today's online world possible.

Based on a publicly trusted certificate, SSL technology was created to help prevent theft, fraud and other criminal activity within the new online frontier. Personal data had to be protected, credit card numbers secured, and transactions safeguarded.

And while SSL technology has advanced since, the understanding gained from its development has helped extend digital certificates to secure all aspects of today's connected world.

## In your everyday devices

An electronic document that is embedded into a hardware device and can last as long as the device is used, a device certificate's purpose is similar to that of a driver's license or passport: it provides proof of the device's identity and, by extension, the identity of the device owner.

Popular examples of devices that are secured by certificates include cable-ready TVs, smart meters, mobile smartphone devices, wireless routers, satellite receivers and others.

Using device certificates helps protect services from unauthorized access, possibly by cloned devices. Typically, an organization injects certificates into devices that are then distributed across a large user base.

## Protecting your identity

A technology that is rarely seen but always relied upon, digital certificates help secure important identity aspects of everyday lives. Specialized digital certificates authenticate identities everywhere from typical office

environments to border security checkpoints.

Also, as the backbone of the ePassport trust infrastructure, PKI and digital certificates help secure domestic and international borders by implementing technology that makes it difficult for criminals to duplicate, deceive or circumvent identity documents.

### Securing the machines

By issuing certificates to machines, organizations permit authorized machines to access a network by authenticating to other machines, devices or servers — typically in either Microsoft Windows or UNIX environments — using a certificate. This allows authorized machines to access and share confidential data.

Many other solutions for securing networks, including firewalls or network isolation (which prevents access to the Intranet/Internet), are either susceptible to attack or are not practical. Using certificate-based authentication for machines is the best way to secure a network.

This approach prevents unauthorized machines from accessing a network; encrypts machine-to-machine communication; and permits machines, both attended and unattended, to authenticate to the network over a wired or wireless network connection.

Typical deployment scenarios include hospitals, law enforcement, government and more.

**As data breaches, identity theft and information loss continue being commonplace occurrences, digital certificates in the enterprise enable organizations to solve security challenges quickly, easily and in a cost-effective manner.**

### Enterprise security

Popular with enterprises, desktop certificates enable secure e-mail, file and folder encryption, secure remote access (VPN) and the secure use of electronic forms and PDFs. As data breaches, identity theft and information loss continue being commonplace occurrences, digital certificates in the enterprise enable organizations to solve security challenges quickly, easily and in a cost-effective manner.

While there are many factors that contribute to the increase of use of digital certificates, one of the most compelling is the widespread presence of mobile devices.

From 8-year-olds to retired grandparents, many people have now access to or use mobile devices daily. And many of those devices are embedded with a digital certificate that authenticates its identity and ties it to the owner.

According to a recent Gartner report, global mobile phone end-user sales grew 35 percent in Q3 2010 over Q3 2009, accounting for 417 million devices sold. The report also noted that smartphone growth increased 96 percent in the third quarter compared to 2009. With many of these brands and models either including digital certificates out of the box or providing the option to install them, the increase in digital certificate use is easy to understand.

Of course, the ubiquity of mobile devices isn't the only catalyst. As digital certificate products and capabilities become available from different vendors, the cost of implementing them decreases.

### Growing pains

But this raises an important question: is it all happening too fast? The answer is yes – in some cases. As organizations rely more and more on digital certificates, they can be overwhelmed with the day-to-day management of large certificate pools.

It's really not an arduous chore if you have only a handful of digital certificates, but many organizations deploy thousands of digital certificates with their products, services and even within the organization itself.

Without a proven system in place, it's easy to lose track of thousands of expiry dates, deployment locations and certificate copies, not to mention errors introduced by the human element.

So, what's the best approach for mitigating these difficulties? To date, one of the most relied upon methods is to employ a two-pronged strategy — certificate discovery and management.

## Certificate discovery

The most trusted and successful security vendors offer certificate discovery services that use network scans to search for certificates on both internal and external hosts. This solution can typically be configured to scan given IP addresses or IP ranges, looking for certificates, with a goal of exposing potential problems on the network.

Certificate discovery solutions often highlight pending issues such as certificates about to expire or certificates from unauthorized vendors.

## Upper management

Once an organization fully understands its certificate environment, it's best to employ a proven tool or service to help streamline the day-to-day management of large certificate pools. These services range from simple (and often limited) software products to robust hosted services that provide more functionality, customization and control.

The more advanced services — whether deployed on-site or realized via a cloud-based model — enable organizations to easily circumvent the issues that plague unmanaged certificate environments (e.g. self-signed certificate creation, certificate copies, expiring certificates, etc.).

## Cryptography and compliance

Organizations that are subject to regulations typically implement a security policy concerning the use of digital certificates. This often results in certificate-reporting and audit requirements. Typically, organizations provide a list of certificates issued from their known CAs to adhere to these requirements. In most cases, however, these lists are incomplete because some CAs are unknown and certificates have been copied.

That might present a problem. An organization's policy might require 2048-bit keys, and it's likely enforced with known CAs. But with unknown CAs, organizations could have weak cryptography deployed and be unaware of the oversight, leaving them vulnerable to a data breach.

The potential presence of unknown CAs or copied certificates also means IT departments cannot provide a complete list of all certificates — leaving an organization non-compliant and at risk during an audit.

## Side with a security expert

As digital certificates become a more critical component in our daily lives, security experts are available to help organizations leverage the technology, regardless of their current deployment status.

Proven security companies are available to help organizations understand which certificates are best suited to meet their business objectives. And they also provide the tools and service to manage all certificates — regardless of type, purpose or environment.

If not properly managed from the onset, large certificate pools can quickly become unorganized. This may lead to higher costs, non-compliance and the unnecessary use of workforce bandwidth. And this doesn't even account for the negative effect that may occur to a brand, product or service in the consumer's eyes.

And even if an organization didn't deploy certificates via a management tool or service, it's not too late to partner with a provider that can help deploy the necessary discovery and management tools to make sense of all digital certificates — no matter how many are deployed.

Scott Shetler is a Product Manager at Entrust (www.entrust.com).


## How to protect your company from social engineering attacks

(www.net-security.org/article.php?id=1545)

Jayson E. Street is the Chief Infosec Officer at Stratagem 1 Solutions, the author of the book Dissecting the hack: the f0rb1dd3n network and a well-known information security speaker. Jayson offers advice for companies on how to prepare themselves for potentially dangerous social engineering situations.

## Today's security landscape: Threats, data breaches and privacy

(www.net-security.org/article.php?id=1498)

Jack Danahy, the Worldwide Security Executive, IBM/Rational at IBM, talks about current threats, data breaches and privacy.

## Secunia's role in vulnerability management

(www.net-security.org/article.php?id=1562)

Secunia CSO Thomas Kristensen talks about the company and their product line. Kristensen tackles the following questions:

• Tell us more about Secunia, and the role of vulnerability research in your organization.
• Secunia offers the Corporate Software Inspector for finding and fixing unpatched endpoints and applications. How is this different from some of the competing vulnerability management solutions currently available?
• Does Secunia see itself competing directly against more traditional vulnerability scanners or patch management solutions with Corporate Software Inspector or do customers consider this to be a complementary solution?
• Secunia also offers the Vulnerability Intelligence Manager and Personal Software Inspector. How do these solutions fit into your product portfolio?

## Securing the enterprise: Insight from Qualys
(www.net-security.org/article.php?id=1567)

In this video, recorded at RSA Conference 2011 in San Francisco, Qualys Chairman and CEO Philippe Courtot talks about the myriad of innovations coming from the company:

• Next generation SaaS platform to host the QualysGuard IT security and compliance SaaS suite of applications in the cloud.
• IronBee - a new open source project to provide the next-generation of web application firewall technology.
• Virtualized software-based scanner appliances for its QualysGuard SaaS IT security and compliance platform.
• QualysGuard WAS 2.0 with several major enhancements to help customers catalog their web applications on a global scale and scan them for vulnerabilities that can lead to exploitation.
• QualysGuard Policy Compliance 3.0, providing more comprehensive policy compliance scanning capabilities without the need to install agents.
• New Trend Micro integrations to help customers more efficiently remediate threats and proactively plan their security strategies.


**While WikiLeaks has reminded all of us that the biggest data security threat always comes from the inside, it should not overshadow the ever-present external threat that are cybercriminals. Given the recent string of high-profile breaches, many CSOs are rethinking their data security strategies.**

Here are five key questions that you need to ask when reevaluating your data security solutions:

1) Is it secure? Will this solution protect my data? This seems like an elementary question, but your solution absolutely MUST be able to address it.

2) How will it affect performance? How will the solution impact the capacity and performance of your critical IT systems, servers, etc.? Will it slow down performance? Make sure your solution allows you to perform day-to-day actions unimpeded.

3) Does it meet PCI compliance? According the Verizon 2010 Data Breach Investigations Report, 79 percent of data breach victims had not achieved compliance. If you are a merchant, payments processor or financial institution with access to payments cards data, you must be PCI compliant.

Nowadays, even the companies that don't have credit card payments as a core part of their business have to worry about PCI compliance because a very small part of their business incorporates some form of payment processing.

If you are one of these companies, you need to ask your data security solution provider if their solution meets PCI standards, and how the solution helps remediate annual compliance costs.

You may find that the security solution makes it easier or more difficult for you to perform your annual PCI compliance audit, so weighing how the data security solution affects costs for your audit is a key issue to think about.

4) Where is it vulnerable? You need to have a comprehensive understanding of your security solution, including how it can be breached and how your data will be protected if it is breached. For example, encryption secures data even in the event of a security breach by using an encryption key which is based on an algorithm. While this is a good step to protect data, if a sophisticated hacker gets a hold of your encryption key or breaks the algorithm to decrypt the data, he will still be able to access your data.

5) How much will it cost? Data security is expensive, but data breaches are more expensive. A recent Ponemon Study revealed that the average cost of a data breach in 2009 was $3.4 million. This number coupled with already excising data security costs will cripple an organization financially. It is important to look at cost when comparing solutions, but data security is one place where most organizations cannot afford to make a mistake.

**THE AVERAGE COST OF A DATA BREACH IN 2009 WAS $3.4 MILLION. THIS NUMBER COUPLED WITH ALREADY EXCISING DATA SECURITY COSTS WILL CRIPPLE AN ORGANIZATION FINANCIALLY**

One emerging data security solution that is getting a lot of attention based on its ability to address all of the above concerns is tokenization. Many argue that it is more secure than encryption because tokenization replaces sensitive data with random tokens that cannot be decrypted.

Since tokenization is not based on a mathematic formula and is completely random once the data is tokenized, cybercriminals can only decode it by obtaining the token and breaking into the tokenization server.

Therefore, even if they hack into a system, they will not be able to do anything with the data. Tokenization is also a powerful solution for companies that are concerned with meeting PCI compliance because the sensitive tokenized data is managed by the outsourced payments processor, not the merchant.

For companies that do not want to have access to the sensitive data so they don't have to deal with PCI compliance, tokenization relieves their servers of being within the scope of PCI compliance.

The PCI Standards Security Council has still not set the standards for tokenization, but they are expected to be released in early 2011. Once these standards are announced, we can expect to see many more enterprises turning to tokenization solutions over encryption.

Ultimately, cybercriminals will always be trying to steal your sensitive data, so it is important to reevaluate your data security solution at least once a year. Be sure to stay abreast of data security trends and emerging technologies, and most importantly, have a comprehensive understanding of your current solution.

Doing so will allow you to be more agile when making necessary modifications and upgrades as data breaches become more and more sophisticated.

---

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology.

**Bagley**

"Independently reviewed by industry experts these free tools proved to be useful for IT pros."

# Top 10 Free Tools for System Administrators

## Audit Active Directory and file servers, detect inactive users, block USB devices, and more – for free.

The following freeware tools by Redmond Readers' Choice Award-winner NetWrix Corporation can save you a lot of time and make your network more efficient – at absolutely no cost. All of these tools also have advanced commercial editions with additional features, but the freeware editions will not expire, and will not stop working when you urgently need them.

1 **Active Directory Change Reporter** (Windows IT Pro Sep'09: InstantDoc ID 102446, TechRepublic: www.tinyurl.com/6c26db6)—This simple auditing tool keeps tabs on what's going on inside your Active Directory. The Windows IT Pro 2010 Community Choice and Editors' Best Award-winner tracks changes to users, groups, OUs, and all other types of AD objects, sending detailed daily reports with lists of changes. Download link: www.tinyurl.com/4bz3mzc

2 **Privileged Account Manager** (SC Magazine: www.tinyurl.com/5rpoufq)—This product maintains a repository of privileged user accounts (such as Administrator, root, service accounts etc) in Active Directory, servers, and other systems, providing a secure web-based portal for role-based access and automatic maintenance of shared administrative user accounts. The Privileged Account Manager can automatically generate strong passwords at specified intervals (e.g. every 30 days) and synchronize password changes on all target systems (for example, change service account password in Active Directory and update service credentials). Download link: www.tinyurl.com/47a7jw9

3 **USB Blocker** (Windows IT Pro Nov'09: InstantDoc ID 102860)—The increasing mobility of flash drives, MP3 players, cell phones and iPods makes the threat of data theft greater than ever, and with a couple clicks of the mouse, this aptly-named tool blocks unauthorized usage of removable media via USB ports. USB Blocker hardens end point security by preventing the spread of harmful malware and restricting the transfer of confidential information. Download link: www.tinyurl.com/45c4l82

4 **Password Expiration Notifier** (Redmond Magazine Feb'09, 4sysops: www.tinyurl.com/6zw3wm7)—This tool automatically reminds users to change their passwords before they expire, helping keep helpdesk administrators safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (VPN and OWA). Download link: www.tinyurl.com/484stxf

5 **Inactive Users Tracker** (MS TechNet Magazine May'08: www.tinyurl.com/6fwoua3, TechRepublic: www.tinyurl.com/67qj5cd)—This tool tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, thus eliminating potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). Download link: www.tinyurl.com/4hnl4e5

6 **File Server Change Reporter** (4sysops.com: www.tinyurl.com/5sr8psv)—This is a must-have tool for auditing file servers and appliances. The tool detects changes made to files, folders and permissions, and tracks newly created and deleted files. The tool is useful for detecting mistakenly deleted files and it allows quick backup recovery of accidental changes. Download link: www.tinyurl.com/4o8zhls

7 **Active Directory Object Restore Wizard** (Windows IT Pro: www.tinyurl.com/6jnkpgb)—This tool can save the day if someone accidentally (or intentionally) deletes important Active Directory objects. It provides granular object-level, and even attribute-level restore capabilities that allow quick rollbacks of unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). Download link: www.tinyurl.com/4etqt3f

8 **VMware Change Reporter** (TechTarget/SearchVirtualDesktop: www.tinyurl.com/6a2ygto)—If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect things that you are responsible for. This 2010 Windows IT Pro Community Choice and Editor's Best Award-winner tracks and reports changes in VMware Virtual Center settings and permissions, such as newly created virtual machines, containers, alerts and more. Download link: www.tinyurl.com/4rp8aew

9 **Windows Service Monitor** (WindowsReference.com: www.tinyurl.com/66bqkpq)—This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The 2010 Windows IT Pro Community Choice and Editor's Best Award-winning tool also detects services that fail to start at boot time, which can happen, for example, with Microsoft Exchange. Download link: www.tinyurl.com/4bkop4w

10 **Disk Space Monitor** (MS TechNet Magazine Sep'09: www.tinyurl.com/68nnvzb)— Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. Download link: www.tinyurl.com/4qqzmow

---

**JOHN BAGLEY** (john_bagley@sbcglobal.net) is an award-winning professional writer and independent consultant, who contributes to newspapers and magazines.

# How to achieve strong authentication on the Web while balancing security, usability and cost

by Roman Yudkin

**In December, nearly 1.5 million Gawker Media group user credentials were stolen and published online. Being aware that many people use the same password on multiple websites, spammers used the stolen Gawker login credentials to inappropriately access accounts on other unrelated websites for the purpose of spreading spam and committing fraud. Amazon, Twitter, LinkedIn and many other websites were forced to send communications to their users, instructing them to change their passwords to protect their accounts.**

This is not the first time that a breach of passwords for a single website created a domino effect that harmed security for other businesses.

When the 2009 data breach of the social site RockYou.com exposed the login credentials of 32 million users, researchers estimated that 10 percent of those login credentials could be used to access PayPal accounts!

The domino effect is caused not only by poor password practices on the part of users, but also by weak security and authentication standards on the part of the websites. A recent study of 150 popular, high-traffic websites conducted by researchers at the University of Cambridge showed that the majority of them have appallingly weak authentication schemes. Once an attacker has access to user accounts – whether through a brute force attack on a website, through stolen login credentials or by guessing users' weak passwords – the negative repercussions can be ruinous for a business and include legal liability, fines, damage to brand reputation, loss of customers, the unplanned costs to improve IT security systems and more.

These high-profile incidents highlight the urgent need for businesses to stop relying solely on passwords for authentication on their public-facing websites, and start implementing stronger authentication models. To achieve this, IT professionals must understand how to strike a balance between security, usability and cost.

## Finding a balance between competing forces

When implementing strong authentication on a website, IT professionals must find a balance among three separate forces whose goals are often at odds: the cost and security needs of the company, the impact on user behavior, and the motivations of the would-be attacker.

The goal of the business is to make website security as rigorous as possible while minimizing the cost and effort spent implementing security controls. To do this, it must take into account the behavior and motivations of both its users and the attackers.

In most cases, the attacker also conducts a cost vs. benefit analysis and takes a rational, business-like perspective when it comes to stealing login credentials. His goal is to maximize profits while minimizing the cost and effort spent achieving the payoff. The more the attacker can do to automate the attack or make its effect widespread, the better the cost vs. payoff becomes. That is why key-logging malware and botnets are still the most pervasive threats, while more sophisticated man-in-the-middle attacks remain rare.

Lastly, the users also instinctively perform their own evaluation of costs vs. benefits and behave in a rational way as a result. Although it's easy to blame the users in a case like the Gawker incident for choosing weak passwords or using the same password on multiple websites, the reality is that creating a unique, strong password for every website one registers with is not a rational choice.

The cognitive burden of remembering so many complex passwords is too high a cost to the user – especially if the user believes the odds of their credentials being stolen are small or that the business behind the website will absorb any losses resulting from fraud. Thus, all the security advice about choosing strong passwords and never re-using them is rejected as a poor cost/benefit tradeoff. It's no wonder then that users continue to have bad password practices.

The motives of the business, the user and the attacker are often competing but they are all intertwined and IT security professionals should not think of them as separate islands of behavior. We must consider them all when developing an effective security strategy.

The goal is to achieve the optimal balance of security and usability – that sweet spot where you have optimized the cost/benefit tradeoff for the business, made the security requirements easy enough for users to adhere to, and made it just difficult enough for the would-be attacker that it is not worth their effort and they seek a different target.

So, how do we find that sweet spot?

**The more the attacker can do to automate the attack or make its effect widespread, the better the cost vs. payoff becomes.**

## Recommendations

As the Gawker breach showed, the security of a company's website is affected by the security of every other website. You can't control the security practices at other companies, so you must implement measures to identify risk, add layers of authentication, and incorporate one-time passwords to stop the domino effect from spreading to your company's website.

For some businesses, true multifactor authentication will be necessary. Many others will be able to greatly strengthen authentication with some simple-to-implement security improvements. The key is to understand the security needs of your organization and consider the following recommendations with that understanding in mind.

**Evaluate your business needs and consider the most common security threats:** First, consider the industry in which the business operates. What type of data needs to be protected and why? What form would an attack most likely take?

(e.g. Is an attacker likely to steal user credentials and sell them for profit, or more likely to use stolen credentials to access user accounts and commit fraud? Are you most concerned about stopping brute force attacks, or could your site be a target for a more sophisticated threat such as a man-in-the-middle attack?)

Are there data security regulations with which the company must comply? Who is the user population – are they employees, business partners or the general public? How security savvy is the user population?

Evaluate your business needs and consider the most common security threats: First, consider the industry in which the business operates. What type of data needs to be protected and why? What form would an attack most likely take? Conducting an evaluation of the business needs, the most prevalent threats and the user behavior will help determine the level of risk and how stringent the authentication requirements should be.

Strengthen the existing authentication without placing excessive additional burden on the user. Any website requiring authentication should have at least the following basic security measures in place:

• Enforce a dictionary check on passwords to ensure that the user cannot choose a common word for their password.

• Require a strong username that includes a numeric character. Often the username is the easiest portion of the login credentials for a hacker to guess.

• Limit the number of failed login attempts. If a user fails the login three times, temporarily suspend the account until they authenticate through other means.

• If login failed, don't identify which user credential is incorrect. Stating that the 'password is incorrect' or the 'username doesn't exist' allows hackers to harvest existing account information. A general statement such as "Incorrect login, please try again" helps prevent account harvesting.

• Use SSL to create an encrypted link between your server and the user's Web browser during account enrollment, the normal login process and the password reset process.

• Provide the user with contextual advice on how to choose a strong username and password. Research shows that users do choose better passwords when given advice on how to do so.

These steps may seem rudimentary to some readers, but the Cambridge study cited previously showed that only 16 percent of sites limited the number of failed login attempts, only 9 percent conducted a simple dictionary check to prevent "password" from being the password, and only 2 percent of the sites hashed the user's password in JavaScript running in the browser to prevent the server from ever receiving the users' clear text password.

Add additional layers of authentication for higher risk situations. Use behavioral and contextual risk profiling tools and techniques to dynamically trigger additional layers of authentication.

Identify device reputation, and evaluate the geolocation of the user's IP address and time of day that they are accessing the site. Also examine the frequency of the login attempts, which could indicate a brute force attack.

If a high-risk situation is identified, there are several options for additional layers of authentication that can be used:

**Knowledge-based challenge questions**: Many websites rely on various forms of challenge questions for additional security. However, this method has its own usability and security issues.

For example, the answers to challenge questions can often be discovered by searching a person's online profiles and social networks. Or, the information on which the questions are based can be incorrect, as one Forbes reporter discovered when she failed to pass automated security questions supposedly based on facts from her own life.

**Tokenless one-time passwords:** A better option for an additional layer of authentication is a one-time password. Adding a one-time password to the traditional username/password authentication makes the login credentials unique each time.

This makes the login session secure even if the user chose a weak password or uses the same password on multiple sites. It also stops attackers from logging-in even if they obtained users' credentials from another site or through other means, through social engineering or by using keylogging malware – the most common approaches.

The growth of cloud computing and software-as-a-service (SaaS) now makes it possible to deliver one-time passwords (OTP) without using costly hardware tokens, key fobs or smart cards.

For example, an image-based authentication approach prompts users to identify pictures that fit pre-chosen categories. The pictures are different each time and have random alphanumeric characters assigned to them, which form a one-time password when the user identifies the correct pictures. On-screen dynamic keyboards have also been used as a method to generate passcodes.

SaaS one-time password solutions are well-suited to the business objective of increasing security with minimal cost (no need for hardware or infrastructure integrations) and are easy for the user (no need to carry tokens), making it more likely the user will adopt the stronger security practice.

While one-time passwords won't stop a more sophisticated, man-in-the-middle attack, they do stop many of the most common threats – making the effort difficult enough that most attackers will seek an easier target elsewhere.

**Multifactor authentication:** Organizations requiring an even greater level of security should implement true multifactor authentication, which must include at least two of the following factors:

- Something the user knows
- Something the user has
- Something the user is.

**The widespread use of mobile phones has made implementing multifactor authentication easier and more cost effective than in the past.**

**Mobile phones:** The widespread use of mobile phones has made implementing multifactor authentication easier and more cost effective than in the past.

The business sends a one-time passcode to the user's phone via SMS text message and the user types the code they received into the web page to authenticate. The user likely always has their phone with them, and the business avoids the cost and effort of buying, distributing and maintaining tokens or smart cards.

A drawback of delivering a one-time passcode by text message is that it's delivered in clear text. If the users' mobile phone has been stolen, a criminal can easily view the message and use the passcode to authenticate successfully.

One way to solve this problem is to deliver a "something the user knows" challenge to the mobile phone rather than a clear text code. For example, the business could deliver an image-based authentication challenge like the one described previously as an MMS message or via an application on the smartphone.

The user would need to correctly identify their secret images (something the user knows) on the phone (something the user has) in order to successfully authenticate.

**Biometrics and behavioral biometrics:** Biometrics and behavioral biometrics are becoming viable authentication options. For example, laptops with built-in video cameras can be used for facial recognition. Fingerprint scanners are quite common in mobile and desktop environments.

Smartphone applications can be used for voice recognition. Retinal scanners, palm-scanners and ear-scanners have all been used in biometric identification. However, drawbacks of biometric authentication include the need to maintain the equipment and 'body parts' to get accurate readings; biometric id data must also be stored in databases and is, therefore, susceptible to malicious theft and forgery.

Use of behavioral biometrics in authentication has been gaining in popularity. Behavioral biometric techniques include software that tracks the user's behavioral patterns such as keystroke speed and mouse movements. It has been demonstrated that these and other behavioral profiling techniques can help to successfully identify an individual user, especially when used as an additional authentication factor.

## Conclusion

Authentication standards on most websites are woefully lacking. Relying solely on username and passwords puts the business, its users and its valuable information at risk. Not every business needs true multifactor authentication, but most businesses can benefit from implementing relatively simple security controls, such as adding one-time passwords. To develop the right authentication strategy, IT professionals must evaluate the security needs of the company and balance the cost/benefit tradeoff of stringent security with the impact on usability and user behavior, while thwarting the objectives of the would-be attacker.

User education is also critical for improving authentication security. Unless the user clearly understands the reasons for and personal benefits of additional authentication requirements, they will find ways to circumvent the policies.

Finally, it's important to remember that 'security' is a process - IT professionals must continually re-evaluate the company's security needs, identify areas for improvement and make a security roadmap for future improvements. Incident response is critical – always have a contingency plan in place to help mitigate the damage as quickly as possible.

The website can never be 100% secure, but IT professionals should aim to be in the optimal zone that balances the costs with the benefits, helps its users and is strong enough to deter most attackers.

Roman Yudkin is the CTO of Confident Technologies (www.confidenttechnologies.com).