CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

BRAVE NEW WORLD OF GLOBAL EAVESDROPPING & ZERO-DAY MALWARE GALORE

SEPTEMBER 2013

CONTENTS

CYBER WARNINGS

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR

PierLuigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

CDTL - LAB REVIEWS

Stevin Victor
stevinv@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Pierluigi Paganini
Dave Porcello
Phillip Hallam-Baker
Christian Mairoll
Anoop Michael Victor
Dan Ross
Edward A. Adams
Peter Jenney
Paul Paget
David Rosen
Allan Cowen
Meisam Eslahi
Mike Danseglio
David Strom
Jeff Bardin
Jake Sailana
Marcela De Vivo
and many more…

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Magazine: http://www.cyberdefensemagazine.com

Executive Producer: Gary S. Miliefsky, CISSP®

Brave New World of Global Eavesdropping and Zero-day Malware

While we all look to the future with RSA Conference 2014 just around the corner next February, we still have lots to do. It seems major world powers from the USA's NSA to the Russian KGB to China's dedicated Cyber-Red Army, all want to spy on all of us, all the time. For what purpose? Leverage? Control? Power? Yes, to all of the above. This brave new world order of global eavesdropping seems to stem from a paranoid approach and lack of trust not only of competing Nation states but of their mutual citizens. In addition, these new forms of Eavesdropping, ranging from spying on Google emails and search results to leveraging products and services like Facebook among others has only taxed and damaged the Internet as well as the trust in its usage. The idealogy that you can find a needle in a trillion byte haystack seems ludicrous – yet unchecked – government entities have decided to create systems to allow them to eavesdrop on everything possible.

Now, instead of empowering others to move to the cloud or to leverage so much mobile horsepower, we now have to worry about our geolocation, our conversations lack of privacy – ultimately a complete lack of respect by world governments. When Putin starts talking about the US eavesdropping program being unbelievable and whistleblowers like Snowden run for safety into the arms of Mother Russia, one has to ask, has the world been turned completely upside down? We keep finding Advanced Persistent Threats and Zero-day Malware being developed solely for the purpose of eavesdropping – this is unheard of – where past malware was almost always made by cyber criminals for the purposes of identity theft, costing banks Billions of dollars in losses accrued, with in-country citizens suffering from these breaches and needing new bank accounts, debit and credit cards. This new malware is truly a new wave of "Spyware".

With that all said, now is the time to learn about the best practices, tools and techniques to protect your own privacy and that of your organization. Vigilance is ever so critical.

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief, Pierluigi.Paganini@cyberdefensemagazine.com

P.S. Congrats Robert Waterman (USA) – this month's contest winner!

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

SAVE $700
BY NOVEMBER 15

Get More in 2014

Elevate your status within your industry. Share ideas with other experts in your field and build your professional network

Gain skills you can actually use on the job. 1 NEW track: Analytics and Forensics, plus MORE tutorials

Access the latest security technology. Explore our BIGGER Expo with 350+ companies

2 Expos
350+ Innovative Exhibitors
280+ Informative Sessions
21 Essential Tracks
5 Days of learning and discovery
1 Premier information security event

FOLLOW US ON: #RSAC

Register Now! www.rsaconference.com/cyberdefense

Global Diamond Sponsors: Juniper Networks, Microsoft, RSA

Global Platinum Sponsors: Cisco, FireEye

Global Gold Sponsors: Akamai, ixia, splunk>

Platinum Sponsors: HP, McAfee, Qualys, Symantec

Gold Sponsors: HOB, SOPHOS, IT Security, Trend Micro, websense

Pwnie Express

Pwn Plug R2

Introducing the Pwn Plug R2: a tightly-integrated penetration testing platform in a portable, shippable, plug-and-pwn form factor.

With onboard high-gain wireless and dual-Ethernet, external high-gain Bluetooth, 4G/GSM cellular, more storage, and many software improvements, the Pwn Plug R2 is the enterprise pentester's dream tool.

HARDWARE SPECS:

- *Processor / RAM: 1.2GHz Armada-370 CPU / 1GB DDR3*
- *Disk storage: 32GB microSDHC*
- *Onboard wireless: High-gain 802.11b/g/n, packet injection & monitor mode, 8" antenna*
- *Onboard I/O: 2x Gigabit Ethernet, 2x USB 3.0, serial console, microSD slot*
- *External high-gain Bluetooth adapter (up to 1000' range) supporting packet injection & monitor mode*
- *Optional support for Zigbee/Zwave, RFID, and Software-Defined Radios (SDR)*
- *Voltage: 110-240v*
- *Power draw: 5 watts idle, 15 watts max*
- *Dimensions: 5.2" x 3.7" x 0.8"*

pwnieexpress.com
sales@pwnieexpress.com
855.793.1337
@pwnieexpress

Core Features

- Onboard high-gain 802.11b/g/n wireless
- Onboard dual Gigabit Ethernet
- External high-gain Bluetooth adapter (up to 1000')
- External unlocked 4G/GSM cellular adapter (SIM card not included)
- 32GB microSDHC disk storage
- Automated NAC/802.1x/RADIUS bypass
- Simple web-based administration with "Pwnix UI"
- One-click Evil AP, stealth mode, & passive recon
- Out-of-band SSH access over 4G/GSM cell networks
- Maintains persistent, covert, encrypted SSH access to your target network
- Tunnels through application-aware firewalls & IPS
- Supports HTTP proxies, SSH-VPN, & OpenVPN
- Runs Pwnix, a custom Debian distro using the Kali Linux (kali.org) repositories
- OSS-based pentesting toolkit includes Metasploit, SET, Kismet, Aircrack-NG, SSLstrip, nmap, Hydra, w3af, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools, & many more!
- Unpingable and no listening ports in stealth mode

Simplifying and Ensuring Data Security Across the WAN

By Keith Ross

A number of forces drive the need for increased data security, including protecting corporate information and trade secrets, government regulation, trade partner privacy agreements, and customer expectations.

For example, in banking and finance, the payment card industry has very strict digital security standards to prevent credit card information from being stolen from the network. The healthcare industry has regulations, including HIPAA and HITECH, to insure that sensitive personal health information is secure.

Current solution: the VPN tunnel

Many organizations don't encrypt their data over the WAN because it's traveling on a "safe" multiprotocol label switching (MPLS) network. Although MPLS networks provide more reliable connections than the Internet and aren't as public, they cannot be counted upon to be private—they're still vulnerable to attack.

It is important to understand that VPNs and technologies such as MPLS are not encrypted by default, and so require additional security measures to protect data. Even if the network is "private" or "virtually private," it is still subject to attacks. Data sent on MPLS networks is kept separate from other traffic, but it is not encrypted. What's more interesting is that over the past few years, many MPLS carriers have merged their private WANs and Internet backbones, further reducing security in the process.

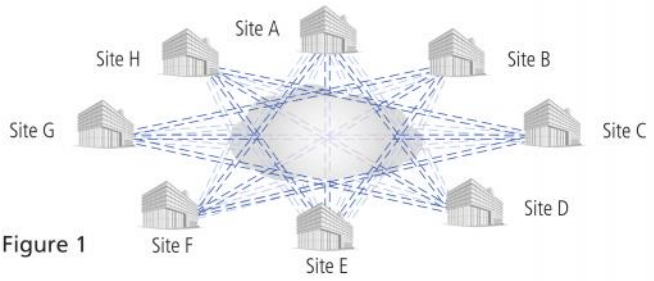


Figure 1

Breaking out of the tunnel

IPsec VPN tunnels are fairly simple to set up between only two points. However, when remote sites multiply, the number of tunnels increases exponentially. A tunnel is needed between each pair of sites **(Fig. 1)**, leading to administrative hassles every time a remote site is added. EncrypTight™ eliminates the need to establish point-to-point tunnels between each pair of remote sites, freeing network administrators for other tasks. With EncrypTight, every site on your WAN can establish an instant encrypted connection to every other site equipped with an EncrypTight appliance.

How is EncrypTight different than a VPN?

The EncrypTight solution is based on group encryption in which the encryption keys are centrally generated and securely sent to the EncrypTight appliances. This enables you to manage policy and key distribution centrally instead of on a time-consuming, site-by-site basis, as is the case with VPNs. EncrypTight enables you to secure "data in motion" in a way that is transparent to network architectures and protocols. And, if you decide to migrate to the Internet from MPLS networks using EncrypTight, you don't experience any service interruptions.

Layer 4 encryption

In addition to Layer 2 Ethernet frame encryption and Layer 3 IP packet encryption, EncrypTight offers a Layer 4 payload-only encryption option. Layer 4 encryption offers many advantages, including:

- Ability to pass encrypted data through NAT devices. VPN tunnels, which encapsulate the Layer 3 address, often don't work with NAT.
- Compatibility with policy-based routing and load balancing that require Layer 3 addresses to be intact.
- Layer 4 encryption leaves Layer 3 headers intact, making it possible to troubleshoot a network without turning off encryption.
- Because headers are intact, data looks unencrypted, making it possible to use within countries that restrict encrypted data.

Faster, safer, cheaper

If you want to lower costs and increase throughput, consider EncrypTight. It will enable you to quickly and easily set up a fully encrypted "mesh" that provides high-speed, secure, any-to-any connectivity over any public (or private) network. You can switch from expensive, private WAN links to inexpensive, public Internet connections with much greater bandwidth (**Fig. 2**). Plus, you'll get a fully compliant solution that offers security via encryption and ongoing authentication.

Cost and Throughput Comparison: Going from 10 Mbps to 100 Mbps

Figure 2

For more information, including a free whitepaper titled *Group Encryption: The key to protecting data in motion*, please visit **blackbox.com/go/EncrypTight**

Keith Ross is the Director of Product Management for networking products at Black Box (www.blackbox.com), a leading supplier of IT infrastructure and networking solutions.

StillSecure® Safe Access®

Do you know who's on your network today?

The power of Safe Access

BYOD
- Enforces BYOD policy
- Complements your Mobile Device Manager (MDM)

Visibility
- Two-second pre-connect/post-connect testing
- 2000+ cross-vendor compliance tests

Efficient
- Scalable to hundreds of thousands of endpoints
- Deploy on physical or virtual servers
- Fully functional in about an hour

Control
- Isolate non-compliant endpoints
- Granular guest access controls
- User- and time-based policy controls

www.StillSecure.com
Twitter: @StillSecure
Blog: www.StillSecure.com/blog
Phone: 303.381.3801

File Transfers Don't Have to Be Risky Business

Simplify • Automate • Encrypt

GoAnywhere™ is a managed file transfer solution that improves workflow efficiency, tightens data security, and increases administrative control across diverse platforms and various databases, with support for all popular protocols (SFTP, FTPS, HTTP/S, AS2, etc.) and encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Optional features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption. **Visit GoAnywhere.com for a free trial.**

See for Yourself

Find out why this bank depends on GoAnywhere to automate daily file exchanges with vendors.

GO ANYWHERE™

a managed file transfer solution by LINOMA SOFTWARE

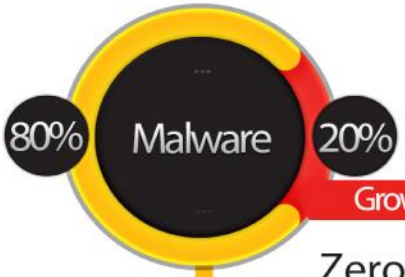
GoAnywhere.com 800.949.4696

SnoopWall

RECLAIM YOUR PRIVACY ™

TRADITIONAL MALWARE

Virus
Blended-Threat
Botnet
Zombie
Worm
Spyware
Trojan



MODERN MALWARE

Growing by 30,000 New Samples Daily

Zero Day
Advanced Persistent Threats
Command & Control Channels
Eavesdropping
Remote Control Threats on Smartphones, Tablets, iPhones & iPads

Anti-Virus programs can detect and protect you from **Traditional Malware** and only a small fraction of **Modern Malware**

SnoopWall protects you from **Modern Malware** - puts you in control

Get SnoopWall for

Windows (COMING SOON!)

iPhone (COMING SOON!)

Android

DID YOU KNOW

Less spying means longer battery life for your devices!

Increase Battery life!

RECLAIM YOUR PRIVACY ™

ZERO NIGHTS

NOVEMBER 7-8, 2013

MOSCOW, RUSSIA

ZeroNights is an international conference dedicated to the practical side of information security.

ZeroNights shows new attack methods and threats, discovers new possibilities of attack and defense, and suggests out-of-the-box security solutions.

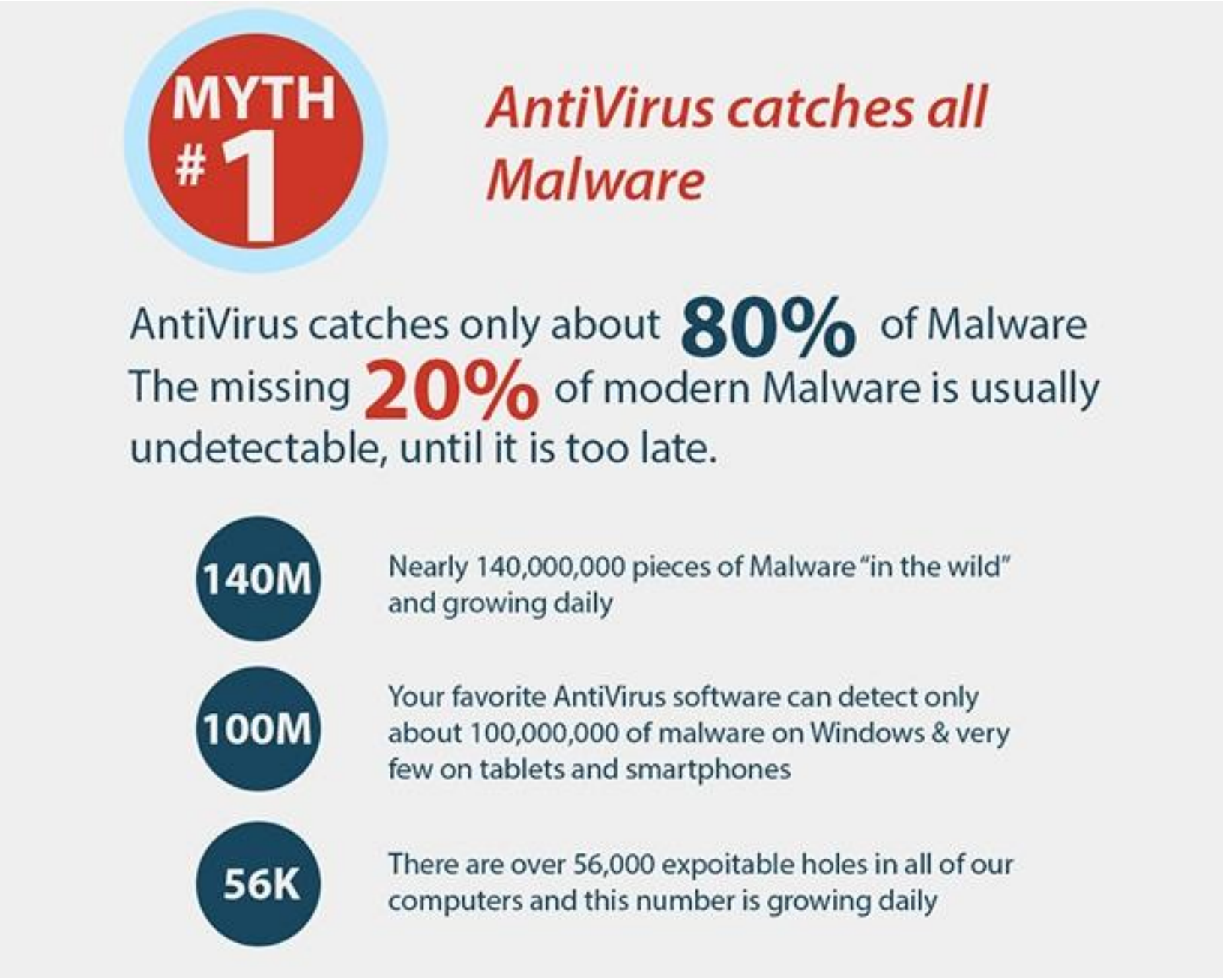
ZeroNights gathers experts, infosecurity practitioners, analysts, and hackers from all over the world.

www.zeronights.org

TWO DAYS OF TECHNICAL SATURNALIA!

Top 3 Myths About Antivirus Software

by AntivirusTruth.org



AntiVirus is proactive

AntiVirus is a **reactive** technology

not proactive.

It cleans up only the malware it recognizes and usually after the infection

Modern malware is going mobile and cannot always be detected. Undetectable malware is also called Zero-Day Malware (0day) and Advanced Persistent Threats (APTs) with Remote Control and Data Theft Through Command and Control (C&C) Channels over the Internet.

(Source: CDM, www.AntiVirusTruth.org, www.privacyrights.org, and nvd.nist.gov)

NSA Spying Concerns? Learn Counterveillance

Free Online Course Replay at www.snoopwall.com/free

"NSA Spying Concerns? Learn Counterveillance" is a 60-minute recorded online instructor-led course for beginners who will learn how easily we are all being spied upon - not just by the NSA but by cyber criminals, malicious insiders and even online predators who watch our children; then you will learn the basics in the art of Counterveillance and how you can use new tools and techniques to defend against this next generation threat of data theft and data leakage.

The course has been developed for IT and IT security professionals including Network Administrators, Data Security Analysts, System and Network Security Administrators, Network Security Engineers and Security Professionals.

After you take the class, you'll have newfound knowledge and understanding of:

1. How you are being Spied upon.
2. Why Counterveillance is so important.
3. What You can do to protect private information.

Course Overview:

How long has the NSA been spying on you?
What tools and techniques have they been using?
Who else has been spying on you?
What tools and techniques they have been using?
What is Counterveillance?
Why is Counterveillance the most important missing piece of your security posture?
How hard is Counterveillance?
What are the best tools and techniques for Counterveillance?

Your Enrollment includes :

1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement for passing the Concise-Courses Counterveillance 101 course.

Visit this course online, sponsored by Concise-Courses.com and SnoopWall.com at
http://www.snoopwall.com/free

Iran hacked US Navy Computers

US officials revealed that Iran hacked unclassified Navy computers in recent weeks in an escalation of cyber attacks against US infrastructures.

The Wall Street Journal reported that Iran hacked unclassified US Navy computers, the allegations were made by US officials that consider the attacks of of most serious intrusion within Government Network made by foreign states.

"The U.S. officials said the attacks were carried out by hackers working for Iran's government or by a group acting with the approval of Iranian leaders. The most recent incident came in the week starting Sept. 15, before a security upgrade, the officials said. Iranian officials didn't respond to requests to comment."

US officials sustained that Iranian hackers working for the government of Teheran have repeatedly violated computer systems within an unclassified Navy computer network for cyber espionage purpose.

Despite no sensitive information has been leaked the event is considered very concerning for US Intelligence, similar attacks could expose confidential information such as blueprints of a new cyber weapon, but could also compromise an architecture of the Defense.

Iran's cyber abilities have increased gradually reaching a concerning level, Teheran has sufficient cyber abilities to attack the US causing serious damages to the critical infrastructures of the country. Iranian state sponsored hackers could hit critical infrastructure using malicious code and tools free available on the internet and purchased in the underground.

The study "*Iran: How a Third Tier Cyber Power Can Still Threaten the United States*", published by the Atlantic Council sustains that despite the Iranian cyber capabilities are considered modest, they could be sufficient to launch attacks against the U.S.that would do more damage to public perceptions than actual infrastructure.

"Their ability to also play in this [cyber] sandbox compounds that concern," a US official said.

US officials added that Congress has been briefed on the attack, Defense Secretary Chuck Hagel and Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey discussed on the necessity further improve government network security.

"The Pentagon wouldn't confirm the alleged Iranian hacks. A department spokesman said its networks are attacked daily. "We take these attempts seriously and work to learn lessons from every one of them," the spokesman said.

"The series of Iranian intrusions revealed a weakness in the Navy network and a shortcoming in the service's defenses compared with other unclassified military networks, according to U.S. officials.

Once the intruders got into the Navy computer system, they were able to exploit security weaknesses to penetrate more deeply into the unclassified network, the officials said."

Iranian state-sponsored hackers already hit US in the past, the US major banks were hit by a series of powerful DDoS attacks and energy industry computer networks were hacked, but if the event is confirmed there is the concrete risk that the cyber conflict may escalate.

Between US and Iran there is a dangerous tension that has repercussions in the cyber space while US President Barack Obama and Iranian President Hassan Rouhani are trying to define a diplomatic conduct to reach an agreement on the development of Iranian nuclear program. The two leaders spoke on Friday, from the White House Friday afternoon, Obama announced he just got off the phone with Iranian President Hassan Rouhani and discussed *"our ongoing efforts to reach an agreement over Iran's nuclear program."*

"I believe we can reach a comprehensive solution," Obama said, adding that he has asked US Secretary of State John Kerry to continue pursuing a deal with Iran that would prohibit Tehran from pursuing the development of nuclear weapons.

"I do believe that there is a basis for a resolution," Obama said.

"Rouhani has indicated that Iran will never develop nuclear weapons," Obama said, hailing that sentiment as a *"major step forward in a new relationship between the United States and the Islamic Republican of Iran."*

The cyber war between US and Iran started a long ago, one of most debated event is the sabotage of Iranian uranium enrichment facilities made with cyber weapon known as Stuxnet.

Cybersecurity experts are not concerned only by Iran, most dangerous players in the cyberspace like China and Russia that have more sophisticated hacking capabilities than Iran.

The conflict between US and Iran is ongoing in the cyberspace and could have serious repercussions on the diplomatic dialogue established between the two governments, a cyber attack could have the same effect of a conventional strike ... this could be just the beginning.

Pierluigi Paganini

(Source: CDM Editor-in-Chief)

CDM Sponsor Spotlight: BlackBox Corporation (NASDAQ: BBOX)

Black Box is a global supplier of IT and networking equipment including solutions for cables and patch panels, cabinets and racks, cooling, power, high-performance KVM, digital signage, AV and multimedia, network testers, datacom, and networking.

The EncrypTight™ data security solution enables organizations to connect multiple sites and secure their data across a public WAN; gain operational efficiencies by eliminating management of a complex mesh of VPN tunnels; and reduce costs by enabling the use of the Internet for WAN transport instead of using more expensive MPLS circuits. EncrypTight supports encryption for Layers 2–4, is compliant with all major data privacy regulations including HIPAA/HITECH and PCI, and provides safe harbor protection. Additional details are available at **blackbox.com/go/EncrypTight**.

Black Box is renowned for 24x7 lifetime technical support, no-questions asked warranties, and award-winning customer service for a broad range of IT products and solutions. Learn more at www.BlackBox.com or contact us at +1 724-746-5500.

5 Key Steps for Securing SCADA Environments

The attack by the Stuxnet virus against Iran in 2010 raised awareness of the vulnerability of industrial systems known as SCADA (Supervisory Control And Data Acquisition), which have been widely implemented across a range of industries for many years. The Stuxnet virus illustrated the urgent need to apply to SCADA environments modern security techniques like those deployed in an enterprise network.

SCADA environments consist of industrial control and management systems - usually deployed on a large scale - that monitor, manage and administer critical infrastructures in various fields such as transport, nuclear, electricity, gas, water... Unlike a company's conventional IT network, a SCADA environment provides interconnection between proprietary industrial systems, such as robots, valves, thermal or chemical sensors, command and control system, and HMI (Human Machine Interface) systems, rather than desktops. While SCADA is mainly deployed in enterprises, it is increasingly being found in private households as well.

SCADA control systems use a dedicated set of communication protocols, such as MODBUS, DNP3 and IEC 60870-5-101 for communication between system elements. These protocols allow control over physical PLC controllers for example, resulting in physical actions such as motor speed increases, temperature reduction etc. For this reason the integrity of these SCADA control messages is paramount and the communication protocols should be fully validated.

Designed for longevity and at a time when cybercrime specifically targeting the industrial sector was not widespread, SCADA systems have not been taken into account within the network security scheme. Because of the isolated nature of industrial systems and the non-existence of interconnection to an IP network, security was not initially considered to be necessary.

However, SCADA architectures have evolved and now robots, measurements systems, command and control tools and remote maintenance systems are all interconnected via a conventional IP network. The problem is not the use of IP itself but rather that they are administered by potentially vulnerable environments, such as the HMI interface platform, which is typically equipped with an unpatched Windows operating system. Considered highly sensitive, these environments generally do not have operating system patches or updates applied for fear of disrupting the industrial system. Often, this fear prevails over the fear of potential IT attacks. Identified as critical, SCADA environments are thus paradoxically less secure and become a potential target for cybercriminals. Once compromised, a hacker would then have full control over the system, as we have seen with Stuxnet, the first discovered worm

that spies on and reprograms industrial systems. This worm exploited Windows Zero Day vulnerabilities - vulnerabilities for which a patch had not yet be developed - and went on to affect tens of thousands of IT systems and one uranium enrichment plant.

Unfortunately, it took a case of an attack the scale of Stuxnet to raise awareness of the potential damage from cyber threats to the industry sector. While traditional computer attacks usually cause non-material damage, Stuxnet brought home the destructive and real capacity of advanced worms and viruses to affect not only corporate data but also water management systems, chemical product production and energy infrastructures.

As a result, industrial companies are starting to integrate security measures into their systems. However, much more is needed before SCADA systems can be considered secure. As a first step, companies deploying SCADA must consider them as part of their overall IT infrastructure, apply the same security measures and techniques that they do for their internal IT infrastructure and get the support from their senior executives for the related additional IT budgets and resources.

Where standards do not exist, industrial companies should follow good practices as defined by the North American Electric Reliability (NERC) or national organizations, such as Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in France. Aside from these, there are other important steps that should be taken to ensure the security of your SCADA environment, considered as sensitive:

- Regular updates

Applying software patches on a regular basis to the SCADA operation system, applications and components is an essential step to avoid security breaches due to vulnerabilities already known by security vendors.

In addition, the implementation of a tool for detection and analysis of vulnerabilities that allows to intercept malicious Internet threats before they impact the network or the target server will enable proactive measures to prevent attacks, avoid service interruptions, and respond quickly and in real-time against emerging threats.

- Partition and isolate the SCADA network

It is essential to isolate the SCADA network from any other corporate network. To that end, the use of DMZ's or bastions will allow you to segment the SCADA architecture. Thus, the HMI network will be separated from robots and measuring devices, supervisory systems, remote control units and communications infrastructures, allowing each environment to be confined and protected from bouncing attacks.

In short, SCADA networks need to be secured in the same way as enterprise networks from malware and intrusion, using Intrusion Prevention Systems (IPS) and anti-malware solutions, which are not just SCADA specific.

- Protocol Validation

After having partitioned and segregated the different elements of a SCADA architecture, the next logical step is to apply protocol validation and control related to its various components. In other words, it is necessary to inspect the MODBUS protocol to be sure it is neither misused nor an attack vector. Also, it is important to make sure that the application that generates MODBUS requests is a legitimate application, which is generated from the right workstation. Thus, application recognition makes sense.

- Segregate administrators from users

In addition to the segmentation of the network, it is crucial to segregate users from administrators and provide different access levels between the two groups. For example, an administrator could have full access, including configuration changes via the HMI, whereas the user may have read-only access.

- Get an overall view of the network

The need for a correlation and event management tool is essential. It is critical that the network administrator has the ability to fully understand the security state of the entire network and for instance know at the same time the robot state, the HMI patch level and its relation to a specific user or component of the architecture.

The generation of security alerts is equally important. By understanding what is happening in the network, the administrator gets the ability to correctly react to network events and take appropriate actions.

The implementation of these steps, although sometimes cumbersome, will ensure that there is a comprehensive security strategy throughout the network and provide an in-depth defense with a security layer at all levels, even at PLC units, for a precise control of exchanges and communications between the SCADA environment and the network infrastructure.

With attacks becoming more sophisticated, like Advanced Persistent Threats (APT), it is critical that industrial organizations realize that integrated security in their SCADA environments is essential if these networks are to continue to function as they were designed to do. By doing so, they should have the ability to control the networks, users and applications, proactively avoiding potential risks. They should also equip themselves with tools designed by specialized teams to identify potential issues in real-time and be able to respond quickly when a threat is confirmed.

About the Author

Richard Henderson is a Security Strategist and Threat Researcher for Fortinet's FortiGuard Labs.

When he isn't researching the latest wave of online threats and malware, he can be found grinding gears through British Columbia's mountain roads or under the hood of his vintage BMW.

DHS Defends Federal and Critical Systems

by Stephanie Sullivan, Market Intelligence Consultant, immixGroup

As the lead for protecting federal civilian networks, the U.S. Department of Homeland Security (DHS) defends both federal and critical systems, such as the electric grid and the dot gov domains. Executive Order 13636 released in February 2013 requires DHS to produce unclassified reports of cyber threats that identify a specific target, as well as establish a process to disseminate those reports. As a means for the agency to accomplish accurate reporting as part of their network security goals DHS awarded its continuous diagnostics & mitigation (CDM) contract late on August 12 to 17 companies for upwards of $6 billion. Awardees include HP, IBM, CGI, Booz Allen, CSC, and SAIC to name a few. BPA awardees will be providing products and solutions from more than 20 additional vendors to combat cyber threats and defend the civilian dot gov networks and critical infrastructure. The General Service Administration (GSA) will run the contract, and will charge a two percent fee for usage. CDM's efforts will defend 17 of the largest federal civilian agencies and DHS itself, and an additional 30 small or micro agencies have expressed interest in DHS putting CDM tools on their network.

If there are no protests that result from the CDM contract awards, then there will likely be a substantial amount of $183 million dollars allocated in the FY13 budget left to be spent in Q4 of FY13 (as long as portions of the funding is not considered multi-year), which only gives DHS two plus weeks of August and the month of September to spend the bulk of that money. In FY14 DHS has requested $168 million dollars for the CDM effort of which $121 million dollars will go towards the acquisition of new products and solutions.

John Streufert heads up the Federal Network Resilience (FNR) office in tandem with his Deputy Director Danny Toler who are both also in charge of the CDM effort. FNR's role is to collaborate across the Federal Government to enhance the nation's cybersecurity posture by providing cyber diagnostics and mitigation services.

Streufert has said that over the next few years we will see the federal government focusing on security controls for networks, packaged software, and, eventually, custom software. Civilian agencies are discussing trying to cover the critical controls in three phases over the next three years for networks and COTS software. According to Federal News Radio there is an additional RFP expected from DHS in collaboration with GSA to award a separate contract for one or more vendors to provide dashboards to collect and present the data pulled from the CDM tools (the solicitation has not been released and is currently under development).

CDM is not the only cybersecurity program within DHS that's making moves late in the FY13 game. The National Cybersecurity and Protection System or NCPS operationally known as Einstein has been focusing on the progress of its current block (Einstein 3), which protects agency computer systems from cyberattacks, specifically being able to detect malicious traffic and proactively stopping such attacks before they can affect vital systems. Bobbie Stempfly, Acting Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), mentioned at the recent Cyber Security Brainstorm session hosted by Meritalk on July 24, 2013 that the first agency (which she would not identify) went live at 7PM July 24 with the first packet of Einstein 3 (to gather perimeter information). Next to move to Einstein 3 will be the Department of Veterans Affairs, and DHS is currently working on installing Einstein 3 on its own systems, but first must negotiate with its Internet Service Provider (ISP).

NCPS requested $406 million in FY14, of which $72 million would be used towards the procurement of new products and solutions. NCPS is an integrated system of intrusion, detection, analytics, intrusion prevention, and information sharing capabilities used to defend the Civilian governments IT infrastructure from cyber threats. Where CDM focuses more primarily on internal threats to the network, NCPS combats external threats.

Other areas of focus for DHS in FY14 include secure information sharing, automating and authenticating applications, as well as placing a continued focus on their workplace-as-a-service cloud offering that aims to provide virtual desktop and mobile device management capabilities. DHS' "Car Wash" is currently in its proof-of-concept phase and aims to provide enterprise-wide mobile device management application process, which will allow the agency to follow applications through their life cycle, including testing, vetting, and validating data, and there will also be a big need for products and solutions to aid in the creation of a cyber kill chain, which will offer the agency a way to measure the success of continuous monitoring in the future.

About the Author

Stephanie Sullivan heads the civilian team in immixGroup's Market Intelligence organization. She is responsible for analyzing opportunities within the federal government to identify enterprise technology segments that fit immixGroup client capabilities. She can be reached at stephanie_sullivan@immixgroup.com.

To learn more about immixGroup, Inc. visit www.immixgroup.com.

F-Secure published Threat Report H1 2013 on security landscape

IT security firm F-Secure has published its Threat Report H1 2013, the document proposes a focus on Java exploits, mobile threats, Bitcoin mining, APTs and Mac malware.

F-Secure security firm has released the Threat Report H1 2013 that provides an overview on cyber security landscape analyzing the events that characterized the first part of the year. The primary cause of incidents according the Threat Report H1 2013 is the unpatched software, in particular Java based applications. In the second half of 2012, around one third of the exploits targeted Java, meanwhile in the first half of 2013 the number of exploits targeted the framework accounted more than half of detected attacks.

The majority of exploit-based attacks are conducted using exploit kits, with 70% of them being attributed to these five: Blackhole, SweetOrange, Crimeboss, Styx and Cool.

The underground market offer for exploit kit development is very prolific, security experts observed that at least one new (or revamped) exploit kit being created each month on average.

"Of special interest this half year: the increasing use of exploit-based attacks facilitated by exploit kits, particularly those targeted against the Java development platform" "The United States and France saw the most exploit-based attacks. Nearly 60% of the Top 10 Detections involved attacks that used exploits, and 80% of those were targeted against the Java development platform"states the report.

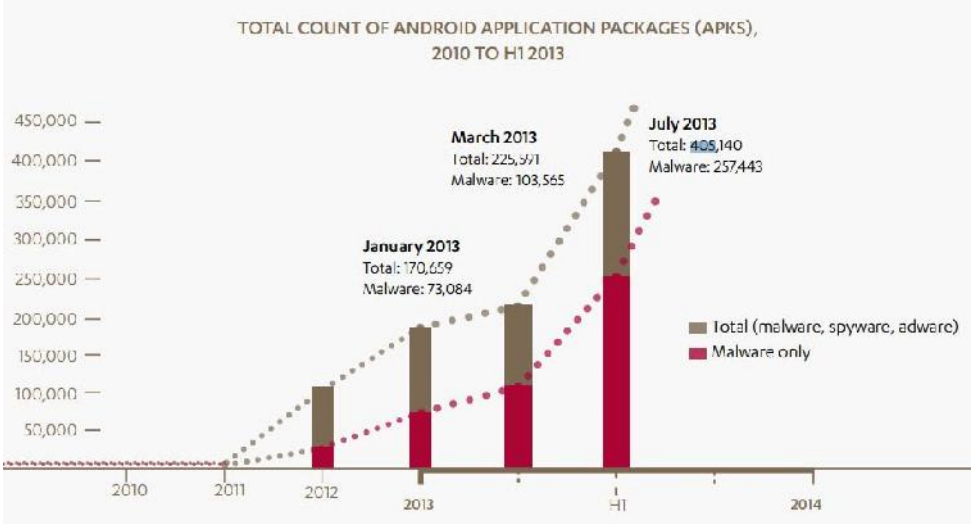
In the following video Mikko Hypponen and Sean Sullivan comment the results of the study.

The Threat Report H1 2013 dedicated a a specific section to the ZeroAccess botnet for which it has been observed a reduction of infections due to increased efficiency in mitigating the attacks. Recent instances of ZeroAccess was used for spreading of a ransomware and to mine Bitcoin. In the following table the estimated profit from ZeroAccess mining activity.

TABLE 1: ESTIMATED PROFIT FROM ZEROACCESS MINING

	USD ($)	BTC (฿)
Daily profit	58,913	585
Weekly profit	412,295	4,095
Monthly profit	1,790,976	17,787

F-Secure confirmed the concerning news from mobile, mobile malware continues to increase and Android was most targeted platform by cybercriminals. In July 2013 the total number of Android application packages containing malicious code that were found is 405,140, over 257,000 contained a malware.



Particular attention is reserved to Mac malware, F-Secure discovered 33 new families and variants in the first half of 2013, the Threat Report H1 2013 reported also of the fist malware signed with a valid developer ID, dubbed Kumar in the Mac (KitM).

I left for last the phishing menace that according the report continues to create serious problems despite the level of awareness reached. Phishing attacks are improved by the use of construction kits now available that simplify the production of phishing sites, phisher are advantaged and can easily spam emails to lure victims onto these automatically created sites, where their personal information and other sensitive information could be stolen.

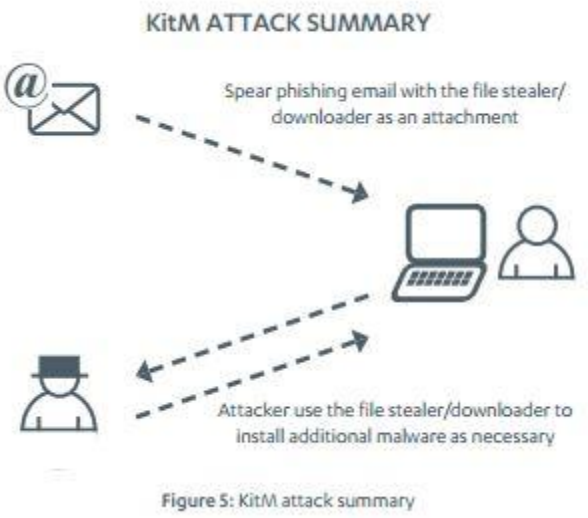
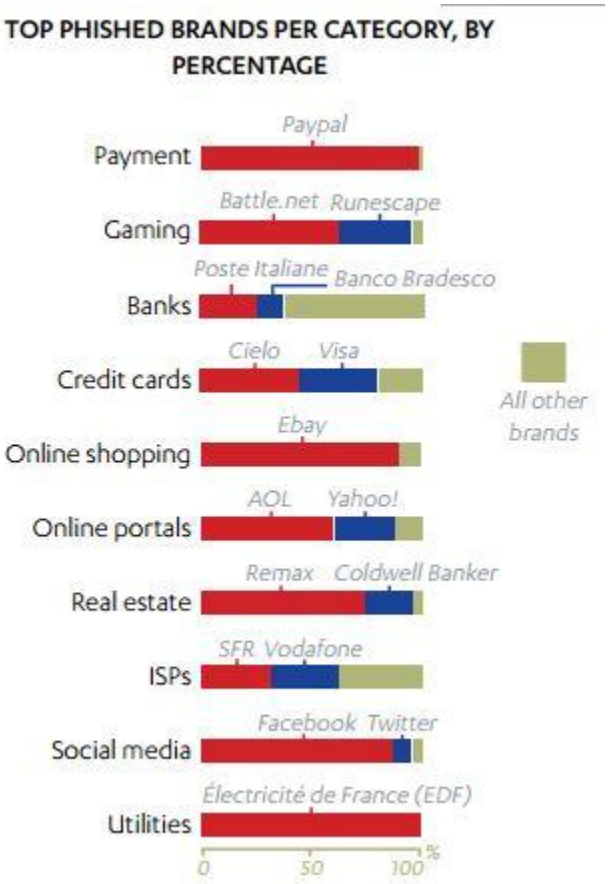


Figure 5: KitM attack summary



The Threat Report H1 2013 provides a collection of case studies on all of the issues discussed in the first part of the document, I suggest its reading.

Pierluigi Paganini

(Source: CDM Editor-in-Chief)

CyberPatriot Continues to Bolster STEM Education

The Air Force Association's CyberPatriot program engages students, parents, and mentors in its sixth season of competition.

By: Caity Rogowski, Communications Assistant, Air Force Association

Since 2009, the Air Force Association's CyberPatriot National High School Cyber Defense Competition has captured the interest of educators, parents, youth program leaders, and students nationwide. The program meets a critical need in drawing young people to science, technology, engineering and mathematics (STEM) education and careers.

Throughout the summer, CyberPatriot staff and other program advocates have promoted the program at a variety of events and conferences related to cyber and STEM education as students nationwide prepare for the upcoming sixth season of competition which begins in October.

"Being able to travel across the country during the summer months gives us many opportunities to excite students, teachers, and parents about our program as they prepare for the upcoming year," said Bernie Skoch, CyberPatriot Comissioner. "We aim to visit areas that already have a strong cyber presence, including San Antonio, CyberCity USA, as well as new places that haven't had a strong CyberPatriot representation in previous competition seasons. We are always on the lookout for the best ways to promote our program and reach out to schools that can benefit from participating in this type of cyber and STEM education."

A CyberPatriot team consists of two to ten students and a coach, but neither coaches nor students need any special technical background. CyberPatriot provides the training materials needed to prepare a team for a successful competition. Additionally, CyberPatriot will facilitate the assignment of volunteer technical cyber experts as mentors to teams who request them. The only cost to teams is a $385 entry fee, which includes access to the software and participant materials.

Preliminary rounds are conducted online from the teams' home locations. The competition has a tournament-style tiered structure, so teams advance based on scores from each round until the top 26 teams are identified. Those top qualifying teams then receive all-expenses-paid trips to the CyberPatriot National Finals Competition held in the Washington, DC area, in March 2014.

Teams also benefit from the expertise of the competition's sponsors, including the Northrop Grumman Foundation, CyberPatriot's Presenting Sponsor, which has contributed mentors, internships and scholarship money to the competition. SAIC is a founding partner of CyberPatriot, along with CIAS at the University of Texas-San Antonio. Other sponsors include AT&T, Cisco, Microsoft Imagine Cup, Raytheon, and USA Today Education.

ALL U.S. high schools or approved home school programs are invited to participate, as are youth organizations such as scouting units, Boys and Girls Clubs, etc. Teams register from public, private, parochial, charter, and home schools in the Open Division, while Junior ROTC units of all Services, US

Naval Sea Cadet Corps divisions, and Civil Air Patrol squadrons compete in the All Service Division. Registration for CyberPatriot VI closes on October 10, 2013, with the first round of competition slated for November 15-17, 2013.

As middle school educators have witnessed the growth of the high school program, they have asked that the program be expanded to include middle school students. In July, the program completed the lead pilot for its upcoming Middle School Program at California State Polytechnic University in Pomona. Through this new initiative, sixth, seventh, and eighth graders from six middle schools in the Los Angeles Unified School District (LAUSD) got the opportunity to learn about cyber safety, basic cybersecurity, and system administration prior to the full Middle School Program rollout, which is schedule for a tiered release throughout the 2013-2014 academic school year.

Students today are making education and career plans sooner than their predecessors. Efforts to shape their choices and draw them in to STEM fields must be done sooner than high school and college. The Middle School Program will focus on equipping students with information they need to understand the importance of cyber systems and how they work, become familiar with cybersecurity principles, and protect themselves on the internet and their mobile devices.

The CyberPatriot Middle School Program will continue to develop as the school year progresses, and the CyberPatriot program looks forward to providing a similar competition curriculum to younger students. “Our Middle School Program is an exciting new addition that will allow us encourage an even younger generation of future cyber defenders,” said Skoch. “Our goal is to introduce as many students as we can to the importance of cyber defense and our nation’s need for a strong support system of cyber leaders in our workforce.” Schools wishing to participate should contact AFA’s CyberPatriot Program Office either by phone 877-885-5716 or by email at info@uscyberpatriot.org.

Participation in CyberPatriot programs has numerous benefits to students and schools. Students are engaged in an interactive curriculum while also focusing on teamwork and competition. The program is designed to promote working towards an end goal, which is ultimately winning one of the top awards at the National Finals Competition. The program goes beyond the competition season by also helping to connect competitors with internships to further their education in the cyber and STEM fields.

CyberPatriot offers students the opportunity to learn real-life skills that they will use in as they further their training and continue on in their professional careers. National security will continue to depend on these professionals as potential vulnerabilities of networks becomes a constant challenge. CyberPatriot’s focus on creating well-rounded cyber defenders will ensure that our country as the trained workforce it needs to identify and rectify potential weaknesses in our network systems.

Presenting cybersecurity within a dynamic and interactive fast-moving competition excites students while exposing them to real world challenges. In each competition round, students are provided one to three virtual machine images. Some of these images will be Windows operating systems, and others will be GNU/Linux. Competitors work to identify and remediate a variety of vulnerabilities within a set amount of time throughout each round.

With nearly 700 teams already registered for CyberPatriot VI, the program is on track for another record-breaking competition season. Participating teams currently represent every state except North Dakota, as well as Puerto Rico, Canada, and Department of Defense Schools in South Korea, and Japan. For more information and to register, visit www.uscyberpatriot.org!

About The Author

Caity Rogowski is the Communications Assistant for the Air Force Association. The Air Force Association is a non-profit, independent, professional military and aerospace education association. Its mission is to promote a dominant United States Air Force and a strong national defense, and to honor Airmen and our Air Force Heritage. To accomplish this, we educate the public on the critical need for unmatched aerospace power and a technically superior workforce to ensure U.S. national security, advocate for aerospace power and STEM education, and support the Total Air Force family while promoting aerospace education. AFA has 200 chapters nationally and internationally representing more than 105,000 members. Caity can be reached online at (crogowski@afa.org, @AirForceAssoc and @CyberPatriot) and at our organization websites www.uscyberpatriot.org and www.afa.org.

How The Information You Share Online Can Put You At Risk For Identity Theft

Social media can at times be a double-edged sword. On one hand, it allows us to connect with our friends and family, stay in touch, market products and even build our businesses; there's no denying that social media divulges an incredible amount of private information, and makes it available to nearly anyone with an internet connection.

Part of the problem is that many users (particularly the young crowds) are ill-informed about the privacy issues surrounding social media, much less how to guard against them.

The good news is that for those of us who want to protect our privacy and still enjoy the benefits of social media, there are some simple precautions we can take to make sure our identity is protected. It doesn't even require that much time or work on your part.

Keep in mind that by simply setting up a social media account, you're opening up at least part of yourself to the general online community. Even a simple Google search can now turn up a web page with your name on it, so right away, we should be prepared to acknowledge that that we're abnegating at least a small amount of privacy.

However, making sure identity thieves won't find those pages the least bit useful is actually pretty straightforward.

Here's where to start:

1. **Avoid posting a full birth date** -- A full birth date by itself isn't useful to an identity thief, but it *is* a piece of the puzzle, especially if they already have your full name.

Display your birthday just by using the month and day. Most people will go this route simply to make sure that friends and family can't calculate their age. There are enough people out there with full birthdays posted, therefore, making them easier targets for identity thieves. Keep your full birth date hidden to avoid giving them more information that they can use to their advantage.

2. **Avoid specific vacation plans** -- Not only can identity thieves take advantage of this, but burglars will actually hire informants to tell them when people are going on vacation. These can just be average people looking in the community: hairdressers, clerks, waiters or waitresses.

That means that it's just a better overall idea to keep the specifics of your vacation plans under wraps, and only inform the people who really need to know. Posting a status update like, "Heading to North Carolina for one week on July 15th!" probably isn't a good idea.

3. **Be vague about where you live** -- Similar to the rule about your birthday, keep your address to a minimum. In fact, keeping it to just the state you live in would be the best solution. Listing your hometown is alright, particularly if it's a big town, but under no circumstances should you list an address or even a street name.

That's valuable information to someone trying to steal either your identity or belongings.

4. **Use privacy settings to filter what people can see** -- Facebook actually has a really robust and highly customizable privacy system that can be adjusted to hide just about anything from anybody. Whether it's

pictures, status updates or the personal information you have listed about yourself, you can hide it from as many or as few people as you want.

Everyone should take the time to get familiar with these privacy settings and adjust them for their Facebook page, especially since Facebook tends to be the most information-rich site.

As a general rule, it's best to keep all information available to just those that are on your friends list.

Minimal Approach

The safest way to deal with online identity theft is to have a minimalist approach when it comes to how much information is revealed, particularly on social networking sites. While you don't necessarily have to starve yourself of the benefits of these sites, just be sure to use best practices and stay intentional about hiding sensitive information.

About The Author

Marcela De Vivo is a freelance writer and online marketing professional who always takes the necessary precautions to protect herself, her family and business from any potential identity theft. She writes for HostPapa to help educate others on how to protect their own information while online.

Continuous Monitoring at the Database Tier

Defending the core is an essential part of a comprehensive cyber security strategy

By Michael Sabo, VP of Marketing, DB Networks

With the advent of continuous monitoring, the era of the annual security audit may rapidly be coming to an end. We are now beginning to close the chapter on this yearly fire drill. It's likely one day we'll look back on this annual ritual and, instead of fond memories, we'll be asking, "what were we thinking"? To be fair the annual security audit did create a forcing factor that motivated shops to finally get that backlog of patches cleared out, find those databases running on the production network that no one remembers creating, and to dust off that circa 1997 disaster recovery plan. But lets be honest, in the vast majority of cases if a security audit weren't a compliance requirement would it really have any priority? Vulnerability assessments and penetration testing will certainly remain necessary periodic events, but the annual security audit is rapidly evolving into a continuous year-round activity rather than a once a year event. Nowhere is this move toward continuous monitoring more important than at the core of the IT infrastructure, the database tier, where the organization's crown jewels reside.

Continuous monitoring is a critical component of the Risk Management Framework (RMF) described in NIST Special Publication 800-37. The RMF stresses the importance of near real-time risk management through effective continuous monitoring. Additionally, the RMF encourages the use of automation to provide the critical information necessary to make cost-effective, risk-based decisions that support the organizations mission. The emphasis is on selecting and implementing proper security controls in conjunction with continuously monitoring. As Dr. Ron Ross, Fellow at the National Institute of Standards and Technology, is fond of saying, "the Risk Management Framework strategy is simple – build it right and then continuously monitor".

All too often in many shops the core infrastructure is simply not "right". Perhaps it was "right" at one time, maybe early on, but over time… As an example, it's common to have unnecessary services running on database and web application servers, to be running applications that expose SQL injection vulnerabilities after a "quick and dirty" patch, to have default passwords active, to have numerous misconfigurations, to be behind on DBMS patches, to not enforce least privileges on database accounts, etc. The core infrastructure should be put "right", stay "right", and then continuously monitored to ensure critical asset protection.

Continuous monitoring at the core may at first appear to be redundant. Is it really necessary to be monitoring for attacks at the core that were intended to be caught at the perimeter? In a nutshell, the answer is yes it is necessary. You absolutely should be continuously monitoring your core infrastructure. The issue is that signature-based monitoring implemented at the perimeter is wholly unsuited to identifying advanced attacks targeting the core. Attackers skilled in obfuscation techniques are able to rapidly bypass perimeter security devices. During an attack if the perimeter security device doesn't recognize the specific attack signature it simply won't alarm. Sophisticated obfuscation techniques are

able to conceal core infrastructure attacks such that they slip seamlessly through perimeter security devices.

Still it's all too common to see perimeter security devices attempting to protect the core. Old habits die hard I suppose. It's also true some compliance specifications simply haven't kept pace with this reality. Once your perimeter defenses have failed you, your "soft core" is then openly vulnerable to cyber attacks. However, continuous monitoring with intrusion detection at the core will immediately identify these breaches. A core IDS, such as DB Networks IDS-6300, provides the security event information necessary to respond to the attack in real-time. In addition, intelligence gathered from continuously monitoring at the core will assist in identifying vulnerabilities in the applications through which the breach occurred. Finally, the more rapidly a security incident can be identified and responded to, the more limited the damage will be. Far better to identify cyber attacks in real-time, while they are ongoing, than during an annual security audit.

About The Author

Michael Sabo is the VP of Marketing at DB Networks. Michael has over 25 years of marketing and strategic planning experience. Prior to DB Networks, Michael was at Intel Corporation where he was responsible for strategic planning. Previously, Michael held senior marketing, business development, and product engineering positions in the telecommunications industry, including at AirFiber, Rhythms NetConnections, US West, and Contel. Michael earned a B.S. in Computer Science from Wright State University and a Masters in Management Information Systems from the University of Denver. Michael can be reached through our company website at www.dbnetworks.com

How Efficient Is Your Vulnerability Management System? Five Questions Every IT Manager Must Ask

By Gidi Cohen, CEO and founder of Skybox Security

Just under the surface of every enterprise network, thousands (and often millions) of vulnerabilities leave an organization's operating systems, applications, network devices, and other critical IT systems open to attack. Vulnerability management plays a critical role in protecting organizations by continuously identifying vulnerabilities, analyzing risks and remediating critical exposures, thus helping security teams limit the exposure to cyber threats by fixing or blocking the gaps with patches, or by tuning the configurations of compensating security controls like intrusion prevention systems (IPS) and firewalls.

Traditional discovery tools like vulnerability scanners can prove disruptive to the network and generate volumes of data with no context or lack clear action items – therefore analysis and remediation can take months to complete. The old-school vulnerability management process is inefficient, especially given that hackers and cyber criminals only need to find a single vulnerability to infiltrate a network. Organizations often must choose between adding more resources to expand an inefficient process or limit the scope of vulnerability analysis and leave the network at risk of potentially devastating cyber attacks.

As next-generation vulnerability management solutions offer a new approach for vulnerability discovery, analysis, and remediation and set a new standard for coverage, speed, and accuracy, security managers need to ask themselves five questions when designing the new process.

1. How Long Does it Take to Get Through a Complete Vulnerability Management Cycle?

In order for vulnerability data to be useful in efforts to patch and safeguard the network ahead of the attack, a vulnerability management cycle – discovery, analysis and remediation – needs to be completed in hours – or a day, at most. Knowing how long it takes your current vulnerability management system to identify, analyze and remediate will help you identify areas for increased efficiencies both in resource requirements and in data timeliness.

Vulnerability scanners require an active scan, which requires a lot of network traffic per test, often resulting in network disruptions. To accommodate, organizations often refrain from frequent scanning and limit scans to well-defined windows throughout the month, quarter or year. With an average scan of 250 hosts per hour, it takes a long time to complete one cycle – typically three months or even longer in a large network – often making the vulnerability data obsolete by the time a complete report is available. Why bother assessing your risks every 90 days when new vulnerabilities are released daily? A next-generation solution can assess vulnerabilities on 90 percent of your network in less than one day, enabling risk analysis and remediation efforts on the most critical risks the same business day.

2. Are You Able to Eliminate High-Risk Vulnerabilities Faster Than New Ones Are Added?

If you don't have the ability to identify vulnerabilities daily and prioritize them by risk immediately, the window of exposure will keep growing. By the time you remediate a critical vulnerability, your network may already have been penetrated. In order to optimize your process, it's essential to have a process that enables daily or continuous vulnerability discovery, as well as quick analysis and remediation.

With the old-school vulnerability management process, far too often IT teams experience information overload when having to manually review three inch thick reports that don't prioritize vulnerabilities using network context. Ultimately, manually looking at vulnerabilities leads teams to remediation that is too late and out of context, and, in many cases, overlooks the most critical ones.

A next-generation vulnerability management solution provides IT teams with actionable intelligence to quickly remediate high severity vulnerabilities that pose the biggest risk to their network. This process is based on the context of the network architecture and a clear understanding of the current security mitigation controls already in place.

3. What is Your False Positive Rate? Double Digits or Less than One Percent?

False positives mean wasted time for IT. If your false positive rate is more than one percent, your staff is spending a lot of time separating relevant risks from irrelevant noise. Vulnerability scanners use a remote probing technique to determine whether a certain service is vulnerable, leading to frequent false positives. In addition, fear of service disruption leads organizations to minimize the set of vulnerability tests they would task the scanner to conduct, which also increases vulnerability data inaccuracy, as real vulnerabilities are not detected.

Examining your current false positive rate will help determine if you have operational inefficiencies, and if so, to what extent. Ideally, you should be experiencing a near zero false positive rate, and this is what you can achieve with a next-generation vulnerability management solution.

4. Have You Been Banned from Scanning Parts of the Network?

To avoid network disruption, many organizations forego scanning the most critical parts of the network, or scan infrequently. Plus, many nodes in the expanded enterprise network cannot be scanned at all, such as mobile devices (especially employee-owned devices), assets in a cloud, SCADA and other operational technology devices. Therefore organizations are left with a tough trade-off between the management headaches of vulnerability scanning and analysis, versus potential cyber attacks inflicted by APTs, malware, cyber criminals, and other sorts of threats.

Next-generation scanless vulnerability discovery techniques identifies vulnerabilities without disrupting critical services, allowing teams to get the vulnerability data they need, continuously, while the network runs smoothly. The scanless approach also provides comprehensive coverage that detects vulnerabilities on critical systems and network devices, such as firewalls and routers and other non-scannable devices.

5. Do You Know What the Biggest Threats to Your Network Are Today?

If your executives ask for your security posture report, do you have the data? We've already reviewed how old-school vulnerability management can take months to complete a cycle from discovery to remediation, making the data obsolete by the time the report is available. So chances are, if you don't have a next-generation vulnerability management process, this is a hard request to fulfill.

With next-generation vulnerability management's automated, metric-driven approach, network teams can continuously analyze, track, and report on risks and the remediation progress on an on-going basis. Having up-to-date insight about cyber security risks and the ability to report on vulnerability data by business unit and platform type is imperative. Plus, it will make you look good.

Conclusion

If your answers to these questions uncover an ineffective vulnerability management process, it's time to raise the current standards to enable a modernized process that quickly eliminates attack vectors to deliver comprehensive and continuous risk mitigation of your IT infrastructure.

About the Author

Gidi Cohen co-founded Skybox in 2002 and has guided the company's vision and development as the leader in cyber security solutions for risk and compliance management. He is a popular speaker at industry conferences, demonstrating how Skybox solutions use risk modeling, network analysis, and attack simulation as practical cyber security tools to predict and prevent potential cyber threats. Gidi holds Bachelors of Science and Master of Science degrees in Computer Sciences and Mathematics from Tel Aviv University.

The Dangers of Spies on Your Keyboard

By Pete Simon, Founder and President of OneForce Technologies

According to the National Cyber Security Alliance, this year and the foreseeable future one in five small businesses in the U.S. will be hacked. Of those that do get hacked, there's a better than 60% chance they will go out of business.

That's about the same odds as playing the game of Russian roulette.

No sane person would ever consider playing that game, knowing the possible end result. So why do small to medium size businesses (SMBs), and many big ones too, play this game in the business world?

Yet all across the globe SMBs, law firms and medical practices play this game on a daily basis with their business computers, leaving them vulnerable to cyberattacks with their sensitive data exposed.

So how do cyber-criminals gain easy access to corporate computers, laptops, and mobile devices? How are they grabbing crucial data that's causing many of the hacked businesses to close their doors for good?

The answer is keyloggers. It's an insidious and extremely effective piece of malware that's capable of evading detection by nearly all anti-virus programs. It can get past sandboxing and white listing attempts by some of the most advanced firewalls and IPS/IDS devices.

A keylogger does exactly what the name states. It captures every keystroke typed on a computer keyboard and transmits that stolen information to a remote server controlled by the hackers. This may seem elementary to many people in the cybersecurity industry, but most people from small business owners up to board members of Fortune 500 companies are not aware of this very effective weapon used to compromise thousands of computer systems.

Keyloggers have been credited with many of the world's most notable breaches: RSA/EMC, Lockheed Martin, Google, Epsilon, Oakridge Nuclear Weapons Lab, Citibank, Sony, World Bank, TJX, Heartland Payment Systems, the New York Times, NBC, Schnucks Supermarkets, as well as tens of millions of medical clinics, small business and consumers around the world.

According to the 2012 Verizon Data Breach Investigative Report, malware was found in 69% of the breaches. Of the breaches where malware was used to steal data, 98% of the time they were paired with keylogging functionality.

Let me emphasize that: 98% of malware contain keyloggers.

What makes the keylogger the preferred weapon of choice is that they have been designed to avoid detection from anti-virus and anti-malware tools, and ephishing training, too. Cyber-criminals continuously test their malware against all the available security solutions to ensure they can evade detection to deliver their payload. Keyloggers can be embedded into any type of download (MP3, video,

a picture file, a codec to run some videos, a Flash file, an online game) or attached to a phishing email or any type of web link.

Speaking of devices, mobile malware has jumped 614% in the last year.

Social Networking websites, like Facebook, LinkedIn, Twitter, Tumblr, and Pintrest, have become one of the favorite places for hackers to propagate spyware. Why? They are porous in terms of defense. Facebook is an extremely popular attack vector because of the popularity of third-party applications and games such as Farmville, Candy Crush Saga, Words With Friends, amongst others. Adding a "dislike" button and apps to see who unfriended you are also very popular and successful tactics. Just last month, a hacker who "debugged" a Facebook code, who wasn't paid, got the world's attention by hacking Mark Zuckerberg's FB page. Should anyone now entrust his or her data on Facebook?

Anti-virus and anti-spyware cannot keep up with this threat; they are still stuck in the 1990s relying on signatures and weak attempts at behavioral analysis. This is why A/V solutions have been found in recent studies and reported in the New York Times to be less than 25% effective against modern malware, and less than 2% effective against a targeted attack. Keyloggers make a mockery of the majority of cyber defenses. It's the path of least resistance for hackers.

The Internal Threat of Email

So what kind of data are the cyber-criminals after that's causing so much economical carnage? For starters, it's banking credentials. Banking websites' usernames and passwords are highly sought after because hackers can easily create wire transfers of all the money in the bank to foreign bank accounts and or prepaid debit cards.

Email user names and passwords are also highly sought after by the cyber-criminals because they are the keys to our online lives. Email addresses can be used to reset passwords for nearly everything we do online, such as credit cards, home utility bills, car payments, health insurance access, and online payroll websites. It's easy for a cyber-criminal to setup several of their cronies with paychecks at the expense of small businesses.

Cyber-criminals are also after product designs, engineering drawings, sales plans / forecasts, negotiation positions, client / customer lists, contracts, sensitive emails, H.R. records with employee social security numbers, and a whole lot more.

For medical practices such as doctor's offices and clinics the danger lies in the fact many of them have poor and non-existent cybersecurity hygiene skills to begin with. They play online games, download music, and surf the web unrestricted on the same computers that house patient medical information. (I know because I have personally witnessed this behavior numerous times.)

Healthcare systems easily become infected with keyloggers due to poor user behavior and protocol, not to mention lack of security tools. Medical office staffs are burdened with finding training solutions and documents to satisfy the HIPAA training compliance and requirements.

In an effort to avoid paying for these solutions, they perform web searches and will download a *free* document, PowerPoint or PDF file. Not realizing that these files may be booby trapped with malware

that was intentionally placed there for free by the hackers in an effort to lure unsuspecting victims to them. This is known as a Watering Hole Attack.

The Prize of Medical Data

Prized medical data includes Medicare and other health insurance identification numbers, access to cloud based EMR/EHR (Electronic Medical Records / Electronic Health Records), access to a doctor's ability to write e-prescriptions. With access to e-prescriptions, a cyber criminal can impersonate a doctor to access expensive drugs and other controlled substances, then invoice them to an unsuspecting patient's insurance. A medical-hacker can also impersonate a patient or obtain expensive medical care under the victim's name.

Medical identity theft is not as easy to repair as financial identity theft. In many cases, these forms of personal attacks take upwards of five years to be corrected, and still might not be done by the credit agencies' indifference towards people. Medical identity theft can also have dire and sometimes-deadly consequences for an elderly or sick victim, with the advent of incorrect prescriptions or treatments as a result of contaminated and altered medical records due to someone impersonating them to obtain healthcare. Is it any wonder that healthcare is seen to be approximately seven to ten years behind the financial industry when it comes to cybersecurity controls?

To think that all of this is started with keyloggers and could have been prevented is the amazing part. Why make life easy for the army of hackers?

Aside from the financial impact of suffering a cyber breach, and/or not reporting it the right way in accordance with data breach notification laws, the damage to reputation can be irreparable. Compound that problem with class action lawsuits, as well as insurance companies denying liability claims to victimized businesses, and state attorney general offices penalizing for suffering a breach. How can these breached companies stay in business?

Over the years many security solutions have sprung up attempting to either stop the keyloggers from getting onto a computer system to using impractical virtual keyboards. Some even give a false and a dangerous sense of security by promising to hold all the secret passwords in an encrypted vault. I say false and dangerous because while the passwords may be encrypted in the database, the master password used to lock and unlock these applications is still susceptible to desktop keylogging.

This is also one of the major flaws of file encryption tools to begin with. What good is encryption if the keys to the kingdom are compromised at the keyboard?

That is an impossible task for these solutions to accomplish because they are attempting to protect the data at the application layer all while the keylogger is operating at the kernel layer hooking into the message queues of the Windows and Apple operating systems (You read that correctly, Apple is not immune to keyloggers). To put it in plain English, they're trying to protect the 7th floor of a building by locking the doors and windows, while completely ignoring the air vents coming up from the basement.

Now this is not an attempt to disparage the password vaults and encryptions tools, because they're still the good guys and are making an effort to combat cyber-crime, except they're fighting the battle on the wrong front.

Many organizations educate their staff with anti-phishing training hoping they become more secure because their employees now recognize the Nigerian 419 scam and know *not* to click on an attachment from a foreign person or entity. But how many of those training sessions are effective at helping an employee recognize that their colleague's or college friend's email have been hijacked by a cyber-criminal in an attempt to get them to open a trapdoor attachment named "executive pay summary" or "recruitment plan"?

That type of spear phishing campaign is what compromised RSA's systems with keyloggers and gave the hackers access to the company's SecureID two-factor authentication product design. A security company being hacked with its flagship product, how ironic is that? Anti-phishing training isn't effective because all it takes is one clueless or disgruntled employee to click on the link and compromise everything. And with large corporations turning over new workers every week, training alone will not get it done.

A company's cyber defenses should never *solely* be dependant on training to detect phishing attempts, which is only one line of defense. Employees should *instead* be trained on what constitutes sensitive and protected information, and how to handle the data to comply with the various regulatory compliance laws. They also need to be trained on the regulatory and privacy laws within the jurisdiction of their businesses, such as HIPAA, PCI, MA201 in the U.S. and the EU Data Protection Act and PCI for businesses that are based or operate within the European Union.

The best approach is a holistic approach. That is what businesses need to survive the relentless assault against all the hard work they've spent years building. The best approach should be comprised of a defense in depth, coupled with education. In other words, focus on protecting the data and applications by locking them down with role based access controls, tag the data to detect abnormal behavior and insider abuse, authenticate the *human* with multi-factor authentication instead of certificates on the machine when a request comes in remotely. And last but not least, cloak the data from the hackers by deploying a "keystroke encryption technology" to render keyloggers useless. Only then will the playing field be leveled and businesses will have a chance of surviving this cyber onslaught.

About The Author

Passionate results driven Information Security Evangelist and IT security solutions architect. Pete Simon founded OneForce Technologies in 2007 with the vision of delivering mobile and enterprise class security solutions to small and medium sized business without the associated price tag and complexity.

Securely Bringing Work to Devices with Containerization

By: Lee Cocking, vice president, corporate strategy, Fixmo

Shifting Your Context from BYOD to BWTD

Organizations are on a mad dash to mobilize existing enterprise data through shiny third party and custom mobile applications. This presents great opportunity, but also introduces significant risk if the appropriate security measures aren't put into place.

Focusing on the security requirements of the data rather than on the devices coming in the door is a subtle, but important, context shift in how we look at the problem of bring your own device (BYOD). We cheekily coined a new acronym to describe this viewpoint – BTWD, or Bringing Work To Devices. Yes, another acronym, and it is meant to be a bit tongue and cheek on purpose, however, the concept reverses the traditional BYOD notion, opining that the question isn't about how you support people bringing their own devices, it's actually about how you bring work to whatever devices happen to be in your environment, in a secure and compliant fashion.

It's a subtle but powerful perspective that changes the focus from devices to the data that you need to mobilize. In other words, it's all about the data. Don't get me wrong, the devices you support are an important factor, but if you start with a data-centric paradigm it's easier to discuss how you want to protect it, then which devices / security mechanisms you need to have in place to do so.

This article will look at each of the different ways you can securely mobilize your application data and support segmentation of business and personal data.

A Look at Containerization Methodologies

Regardless of what you're trying to mobilize, there are quite a few mobile sandboxing (aka containerization) models available to the market today (listed and described below). This may seem like a lot of different categories, but it's necessary to get into the bits and bytes of the various methodologies.

1. <u>OS Virtualization</u>
   - This is your low-level Type 1 Hypervisor or Type 2 virtualization approach.
   - One or more virtual operating systems are created on a single physical device, and either managed by the firmware (Type 1) or a base Host OS (Type 2), where a Host OS is installed, which manages virtualized OS installs above it.

2. <u>Virtual Separation</u>
   - Often the approach taken by Mobile Device Management solutions.
   - Typically a configuration, policy or profile is delivered to a mobile device with instructions to segment certain types of data, usual email.

3. <u>Instancing</u>
   - Instancing can be compared to a typical multi-user environment on a Windows or Linux machine, where one person can log in and see their data and settings, and then later another person can log in and see their own data and settings.

- The segmentation comes from each user having a different 'home' folder where all data and application settings reside.
- In this model, if you launch an enterprise application, it's pointing to and reading your enterprise home folder. Any personal applications that run have no access (based on file / system permissions) to access the enterprise home folder.
- Manufacturer, OEM, or mobile operator customizations are necessary as well. This might look fairly similar to Virtual Separation, however has a system wide focus, as opposed to just controlling certain aspects like email.

4. Virtual Desktop
   - The applications actually run on a server inside your corporate infrastructure, and a thin client resides on a mobile device to drive the virtualized applications.
   - In theory this is a great solution, since you don't need to spend time as an organization rebuilding your apps on a mobile platform, but user engagement and productivity may take a severe hit if you rely purely on Virtual Desktop solutions.

5. Application Space (Layer 7)
   - There's two core sub-segments within this approach: Dynamic Application Wrapping, and the Software Development Kit.
   - Dynamic App Wrapping is a method to take an already created mobile application and dynamically add security controls and policy to it. This is accomplished by manipulating the binary data of a mobile application, which works fairly well for simple applications but has the propensity to fall flat on its face for complex apps.
   - The second method at the application layer is a full on SDK approach, which requires developers within your organization to manually make modifications to your mobile applications.

6. Web Apps
   - A purely web-based approach can be taken by creating web apps, typically in HTML5, which are simply used via a browser on a mobile device.
   - This has the upside of (usually) not storing any data on the device, but the downside (sometimes) of usability and limited security.
   - HTML5 is definitely coming a long way in making web-based applications look and feel like native apps, however it's not 100 percent yet.

Which Methodology is Right for You?

At the end of the day there is no 'best' solution. It's going to depend on a number of factors that will be specific to your organization, and to the applications being mobilized for BYOD. It's very likely that you'll end up supporting a hybrid environment that uses a variety of the methods described, and I think this is perfectly natural given that each app (or piece of data) you mobilize may be for a different user set with different security requirements.

As you set out to decide what solution may work best for you, it is important to take a look at the pros and cons of each model:

	Pros	Cons
OS Virtualization	• Ultra Secure (hard to attack) • Total separation between OS's	• Not widely available (specific devices needed) • Require manufacturer, OEM or mobile operator involvement to customize a specific mobile device. • Usually costly • Very poor strategy for BYOD • Consumes extra resource to run multiple OS's
Virtual Separation	• Wide adoption • Supported by most MDM's already • Easy to deploy • Lightweight	• Poor security – reliant on native OS and extremely vulnerability to Jailbreak / Rooting • Very easy to leak data between business and personal • No extra user authentication
Instancing	• Native support for separation of business and personal data • Minimal extra cost (if any) • More efficient than traditional OS virtualization	• Not widely available (specific devices needed) • Poor strategy for BYOD across the board • Reliant on native protections – vulnerable to jailbreak / root (usually)
Virtual Desktop	• Fairly secure • No data resides on device • Easily mobilize existing systems and thick clients	• Very poor user experience (usually) • No support for native mobile applications
Application Space (Layer 7): Dynamic App Wrapping	• Quick • Easy • Supports many simple applications, including 3rd party • Good strategy for BYOD	• Prone to breaking complex applications • Policy / security controls are high level (if options exist at all) • Encryption (Data-at-rest/data-in-transit) usually weak • Legal issues around wrapping 3rd party applications
Software Development Kit	• Very Secure • Fine grained control over how authentication, encryption, and policy enforcement take place • Great strategy for BYOD • Support for extra integrations with other vendor offered containerized applications (include email, calendar, PIM, browser, and others)	• Manual effort • Source code of application being containerized is needed (difficult for 3rd party applications)
Web Apps	• Quick to mobilize, since all smartphones have browsers • No additional coding effort required • Leverages whatever existing authentication system you've got in place	• Potentially weak transport security • Susceptible to cross-site scripting attacks, cookie attacks, and data exfiltration on device side • No control over cached information, including credentials

Then, there are a few questions you can ask to help narrow down which solution may be the best fit:

1. Who is going to be using the application?
2. What's my timetable to get this application mobilized?
3. What is the level of security required (both for the users and for the data)?
4. What level of extensibility is needed?
5. Is cross-platform support required?
6. Can data reside on the device?
7. Do we require the ability to independently wipe all enterprise data
8. Can we support a device wide VPN or do we need an app level VPN (or equivalent secure transport)?

There is no "right" answer as to the best way to securely mobilize your application data, but hopefully this article has given you some food for thought to help make the decision more well-informed.

About the Author

Lee Cocking, VP of Strategy

Lee is passionate about disruptive technology and an experienced veteran of mobile solutions. He has co-authored several patents on monitoring mobile systems and focuses his time on heading up Fixmo's strategy and product innovation groups. Prior to joining Fixmo, Lee spent nearly a decade at BlackBerry as a member of the support, development and product management organizations, where he worked with leading enterprise mobility customers in both the public and private sectors.

Cyber Warnings Newsflash for September 2013

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Get ready to read on and click the titles below to read the full stories – this has been one of the busiest months in Cyber Crime and Cyber Warfare that we've tracked so far. Even though these titles are in **BLACK**, they are active hyperlinks to the stories, so find those of interest to you and read on through your favorite web browser…

New anti-malware drive focuses on 'EvilGrab'

09/30/2013 03:55 (Computerworld Malaysia)

Trend Micro said EvilGrab is usually launched via spear-**phishing** emails, which presents opportunities for malicious attachments to penetrate...

Week in review: Data broker databases breached, Apple Touch ID hack, and possible solution to click fraud problem

09/30/2013 00:04 (Help Net Security)

...well-known, but is it worth using? Read on to find out. **Phishing** and malicious attachments on the increase Spam volume has dropped in August, but...

UK seeks full cyber warfare capability, experts

09/29/2013 17:24 (Yahoo! Canada Finance)

As governments wage cyber wars, Europe stays away

09/29/2013 15:00 (CNBC)

Europe stays away Governments across the world are engaged in **cyber**-**attack** campaigns against one another, while European administrations have...

Chinese 'Icefog' gang attacks Asian countries using 'hit and run' APTs

09/29/2013 09:29 (Computerworld Malaysia)

...innovative, pivoting on the same collection of tried and trusted **spear**-**phishing** and software exploit via email attacks techniques as every other...

IE zero-day vulnerability exploited more widely than previously thought

09/29/2013 08:52 (Computer World Singapore)

...believe that this is the same group that managed to break into the **computer** network of **security** firm Bit9 as part of a different attack campaign in...

Why the nation needs a US Cyber Force

09/29/2013 01:53 (The Boston Globe)

Why the nation needs a US Cyber Force In the early 1980s **cyber** fiction film, **War** Games, a young hacker played by Matthew Broderick almost managed...

FBI agent fights cyberattacks on corporate America

09/28/2013 20:01 (The Denver Post (AP))

...No. 1 vector of attack for these bad guys is social engineering the **spear** phish, the **phishing** e-mails (aimed at stealing user names, passwords...

Preventing Cyber Security Risks in the Cloud

09/28/2013 04:57 (Technology News)

Preventing **Cyber Security** Risks in the Cloud (PR Web Via Acquire Media NewsEdge) San Diego, USA (PRWEB) September 28, 2013 But the use of a few...

Computer pros advise security programs to prevent hacking

09/27/2013 19:21 (WKBN)

Computer pros advise **security** programs to prevent hacking A California man was arrested for allegedly hacking into the webcams of several women...

Social Media Big Attack Target: IBM Report

09/27/2013 18:32 (Isssource.com)

...X-Force Research and Development team s 2013 mid-year report on **cyber security** trends and risks. The results of the study are from the analysis...

Crime Snapshot: UK Saves a Billion

09/27/2013 17:52 (Isssource.com)

...report 2013. The operations also disrupted 26 national and international **cyber**-based organized **crime** groups and secured 184 years imprisonment for...

LexisNexis confirms data breach; FBI investigating

09/27/2013 15:29 (Bradenton Herald)

...far as April and was first reported by KrebsOnSecurity, a **computer security** blog by former Washington Post reporter Brian Krebs. LexisNexis'

(ISC)² Congress 2013: Financial Market Manipulation Poised as Next Wave in Cybercrime

09/27/2013 11:55 (Infosecurity)

...in Cybercrime Scott Borg, the man who foresaw a Stuxnet-style **cyber**-**attack** years before it was discovered, has issued his latest prediction:

Agencies exploring the right balance between open data, security

09/27/2013 01:39 (FederalNewsRadio.com)

...Health and Human Services is turning to big data to improve the **security** of their **computer** networks. The Department of Health and Human Services...

Challenges faced by top CSOs

09/27/2013 00:54 (Help Net Security)

...challenges they face in making decisions in today s dynamic, turbulent **cyber security** environment. Senior **security** executives, it appears, are getting...

Cybercriminals exploit most news within 22 hours

09/27/2013 00:51 (Help Net Security)

...March 2013, when the new Pope was elected, the first malware and **phishing** attacks began after 55 hours. In April 2013, after the Boston Marathon...

'Viceroi' algorithm improves detection of click fraud

09/26/2013 22:35 (Computerworld Malaysia)

...University of Texas at Austin, will be presented at the ACM Conference on **Computer** and Communications **Security** in Berlin, which will be held Nov. 4-8.

Spear phishing poses threat to industrial control systems

09/26/2013 21:09 (Computerworld Malaysia)

Spear phishing poses threat to industrial control systems **Hackers** don't need Stuxnet or Flame to turn off a city's lights, say security experts...

Digital detectives fight crime with technology

09/26/2013 18:51 (WQOW TV)

Digital detectives fight **crime** with technology Eau Claire (WQOW) - More arrests could've been made this week in an online sex sting if law enforcement...

Tumblr Fixes DOM XSS Bug

09/26/2013 18:20 (Isssource.com)

...issue could end upexploited for spamming, spreading malware and **phishing**, said Portuguese security researcher David Sopas. The vulnerability,

Exec Survey: Attacks Imminent

09/26/2013 17:57 (Isssource.com)

...seem a no brainer, technology and healthcare companies are viewing **cyber security** as a serious threat to their data and business continuity.

Workers Not Thinking Security

09/26/2013 17:49 (Isssource.com)

...opened an email at work they thought was suspicious or a potential **phishing** scam without notifying the IT department, according to the results of...

Beta Bot: A New Trend in Cyber-Attacks - BankInfoSecurity

09/26/2013 16:13 (Bankinfosecurity)

...unique. But Beta Bot is most definitely indicative of the new trend in **cyber**-**attack** vectors." Beta Bot's Attack The Internet Crime Complaint...

Security Staff Feel Largely Unprepared for Cyber-Espionage and APTs

09/26/2013 15:59 (Infosecurity)

Security Staff Feel Largely Unprepared for **Cyber**-Espionage and APTs Advanced persistent threats (APTs) are insidious, multi-pronged and stealthy...

Be Cyber Savvy – October is Cyber Security Awareness Month

09/26/2013 15:01 (DeWitt Media Inc.)

Be **Cyber** Savvy October is **Cyber Security** Awareness Month Are you, your family and your business safe and secure online? Are you, your family...

Icefog: APT Hackers for Hire and Deliveries to Order

09/26/2013 12:31 (Infosecurity)

Japan and Taiwan. The attack method is now fairly typical: **spear**-**phishing** emails that either contain weaponized Word, Excel or HWP documents...

Cyber Resilience: Building a Defense Strategy that Works

09/26/2013 10:51 (Infosecurity)

Cyber Resilience: Building a **Defense** Strategy that Works The ISF s Steve Durbin discusses how organizations can converge cybersecurity and risk...

'Icefog' spying operation targeted Japan, South Korea

09/26/2013 06:28 (Computerworld Malaysia)

...email, sending malicious attachments or links to websites that will **attack** the victim's **computer** if it has software vulnerabilities in programs...

What The Heck is Bitcoin?

09/26/2013 05:58 (Budgets Are Sexy)

...goes beyond just buying a little weed: need to rent a botnet for a **cyber**-**attack**? That can be arranged, as can the purchase of firearms and explosives.

NIST puts finishing touches on critical infrastructure cyber framework

09/26/2013 02:23 (FederalNewsRadio.com)

...three structures: One breaking down five different types of **cyber defense** activity; One addressing various levels of cybersecurity maturity within...

Naval War College professor discusses cyber warfare

09/26/2013 01:21 (Daily Trojan)

Naval **War** College professor discusses **cyber** warfare With WikiLeaks, hacktivism and Internet espionage on the rise, USC s Center for International...

Securing ICS Course at Lambeau Field

09/25/2013 18:23 (Isssource.com)

...Attack an ICS from the Inside-Out o Implementing a **Network** Behavior-based **Intrusion** Detection System for Industrial Control Systems o Network...

Kaspersky Lab Uncovers New Cyber Hit-n-Run Op Called 'Icefog'

09/25/2013 17:58 (Forbes)

...discovered a group of cyber-mercenaries called Icefog . Target: **government** and military institutions. Most of the victims have been in South...

New Virus Hits Freezing Point

09/25/2013 16:51 (Isssource.com)

is responsible for freezing the hard disk. To do this, the **malware** component creates a device that controls the reading and wiring of data on...

Grant to Boost Wireless Security

09/25/2013 16:20 (Isssource.com)

...s principal investigator is Dr. Shucheng Yu, an expert in **cyber security** and assistant professor in UALR s Computer Science Department. Yu said...

(ISC)² Congress 2013: Infosec Must Expand Testing to Keep Pace with Attackers

09/25/2013 13:56 (Infosecurity)

...most organizations believe, and social testing goes beyond simple mock **phishing** tests that some organizations have started to deploy. While not...

Understanding Threats: The Sources

09/25/2013 12:51 (TMCNet)

...Human threats use a variety of methods, including social engineering, **phishing** or pharming, DNS redirection, and botnet operation. An attack...

FBI Issues New Warning on Old Malware: Beta Bot

09/25/2013 11:57 (Infosecurity)

...installation. "Download the latest anti-virus updates or a whole new anti-**virus** program onto an uninfected **computer**, save it to a USB drive and load and...

Looking to the past to combat cyberthreats

09/25/2013 11:08 (The Hill - Blog)

a group of experts released a document, through NATO s center for **cyber defense**, called the Tallinn Manual (named for the Estonian city where...

'Icefog' spying operation targeted Japan, South Korea

09/25/2013 11:07 (Computer World Australia)

...email, sending malicious attachments or links to websites that will **attack** the victim's **computer** if it has software vulnerabilities in programs...

Java exploits jump, Android malware emerges outside app stores

09/25/2013 04:29 (Help Net Security)

...2013, which saw its share of interesting developments in the world of **digital security**. A continued rise in exploit-based attacks, particularly against...

Reactions from the security community to iOS 7

09/25/2013 04:13 (Help Net Security)

...do harm. For example, details could be used to personalize **spear phishing** campaigns to spoof the user into believing the message is legitimate...

Most tech executives planning for cyber attacks

09/25/2013 03:28 (Help Net Security)

...for cyber attacks The majority of technology and healthcare companies view **cyber security** as a serious threat to both their data and business...

Digital watermarking researchers secure more funding

09/25/2013 02:30 (ComputerworldUK.com)

...Research Centre at Ulster s Magee campus, have developed **digital** watermarking technology to ensure the **security** of transmitted data through hidden...

Phishing and malicious attachments on the increase

09/25/2013 02:12 (Help Net Security)

Phishing and malicious attachments on the increase Spam volume has dropped in August, but with the level of **phishing** increasing tenfold and malicious...

Apple is a tempting phishing target for scammers

09/24/2013 22:13 (Computerworld Malaysia)

Apple is a tempting **phishing** target for scammers Spam levels fell in August, but **phishing** attempts rose, including a focus on Apple, according...

Cyber Security Building Block

09/24/2013 17:03 (Isssource.com)

Cyber Security Building Block You can t secure what you don t know you have. You can t secure what you don t know you have. The problem is there...

CISOs Struggle to Keep Up with Mobile and Social Networking Threats

09/24/2013 16:33 (Infosecurity)

...areas account for more than 55% of all scam and **phishing** incidents. While attackers continue to optimize their operational sophistication, a...

Is Fake iMessage App Malware or Not?

09/24/2013 16:32 (CIO Today)

"It's hard to know if it's a bad application or a **phishing** attempt. They're not informing users that their credentials and messages are likely...

Attackers sharpen skills: What that really means for CISOs

09/24/2013 09:52 (Help Net Security)

...to reach more technically savvy victims who may not be fooled in **phishing** attempts, but would not suspect that sites they trust could be malicious.

Survey highlights ignorant IT behavior in the workplace

09/24/2013 09:24 (Help Net Security)

...opened an email at work they suspected to be fake or a **phishing** scam without notifying the IT department according to the results of a survey...

Longwood cyber center earns U.S. designation

09/24/2013 00:00 (Richmond Times-Dispatch (AP))

designation Longwood University has been designated a National Center of **Digital Forensics** Academic Excellence by the **Defense Cyber Crime** Center,

Major increase in Filecoder malware

09/24/2013 05:55 (Help Net Security)

Major increase in Filecoder **malware** The ESET HQ **malware** research lab is reporting an unusual spike in the actvity of Filecoder **malware** - Trojans...

Concerns around insider threats escalate

09/24/2013 05:45 (Help Net Security)

...Principal Analyst at Enterprise Strategy Group. While APTs and advanced **malware** attacks continue in the headlines, the ESG research indicates that...

Twitter fixes Tweet button issue that downloaded a torrent file

09/24/2013 01:29 (Computerworld)

...files are not malicious, but hackers have been known to disguise **malware** by making their program looks like legitimate files in the hope that...

Apple is a tempting phishing target for scammers

09/24/2013 00:32 (Computerworld)

Apple is a tempting **phishing** target for scammers Spam levels fell in August, but **phishing** attempts rose, including a focus on Apple, according...

Security org raises Internet threat level after seeing expanded IE attacks

09/23/2013 23:02 (Computer World Singapore)

...unpatched vulnerabilities. Because Metasploit is a resource for both **security** professionals and **cyber** criminals, the appearance of an exploit...

iPhone TouchID fingerprint biometrics broken by German hacker club

09/23/2013 22:05 (Computer World Singapore)

...that fingerprint biometrics in passports is a poor practice in terms of **security** gains. The Chaos **Computer** Club went on to say that iPhone users...

Java exploits seen as huge menace so far this year

09/23/2013 22:00 (Computerworld Malaysia)

...Another security threat to be reckoned with in the first half of 2013: Mac **malware**. F-Secure reports it saw the "first Mac **malware** signed with a...

DoE Awards to Boost Security Tools

09/23/2013 18:17 (Isssource.com)

...better protect the nation s electric grid, oil and gas infrastructure from **cyber attack**. Eleven **security** vendors earned a share of the $30 million...

Encryption Ransomware Targets Businesses

09/23/2013 17:46 (Isssource.com)

...CryptoLocker, or Trojan:Win32/Crilock, the files targeted by this **malware** are not ones home users might consider important, said researchers at Emsisoft.

Feds: Security Not Sufficient

09/23/2013 16:45 (Isssource.com)

Feds: **Security** Not Sufficient Federal **cyber security** professionals lack confidence in the United States Federal Information Security Management...

Why Antivirus Software Isn't Enough To Fend Off Attacks

09/23/2013 16:07 (Forbes)

...To Fend Off Attacks By Sue Poremba Popular wisdom has long been that no **computer** is safe without anti-**virus** (AV) software installed. By Sue Poremba...

Dept. of Military Affairs: Be cyber savvy: October is Cyber Security Awareness Month

09/23/2013 14:43 (WisPolitics.com)

Dept. of Military Affairs: Be **cyber** savvy: October is **Cyber Security** Awareness Month Contact: Tod Pritchard, WEM Office:(608) 242-3324 Cell:

A short overview of Android banking malware

09/23/2013 14:29 (Help Net Security)

...mobile version is a very recent addition to the group. It spreads via **phishing** emails and, it's interesting to note, tries to infect Android...

Phishing, spoofing, scamming – by any name, it's fraud

09/23/2013 13:03 (Newsmagazine Network)

Phishing, spoofing, scamming by any name, it s fraud The phone call starts innocently enough. The phone call starts innocently enough. A cheerful,

Simulated Attacks Will Test Responses - BankInfoSecurity

09/23/2013 09:01 (Bankinfosecurity)

Simulated Attacks Will Test Responses - BankInfoSecurity **Cyber**-**Attack** Drill to Help Assess Defenses Dennis Simmons ACQ Subscribe More than 1,000...

Federal cyber security pros lack confidence in FISMA

09/23/2013 08:31 (Help Net Security)

Federal **cyber security** pros lack confidence in FISMA A report by MeriTalk and NetApp examines the state of **cyber security** at Federal agencies...

BLOG: Don't let fingerprint sensors leave you in the dark

09/23/2013 05:07 (Computer World Singapore)

...data that can be unintentionally shared. Users are also susceptible to **phishing** attacks, which are the most effective type of attack launched on...

German hackers say old technique can bypass Apple's Touch ID

09/23/2013 05:07 (ComputerworldUK.com)

...(CCC), which hosts an annual hacking conference and publishes **computer security** research, wrote on its blog that their experiment shows that...

Week in review: Undetectable hardware Trojans, Chinese hackers for hire, and latest IE 0-day insight

09/23/2013 00:25 (Help Net Security)

...find the best student teams for the tenth annual NYU-Poly **Cyber Security** Awareness Week. Rootkit freezes computers' hard disk to respawn itself...

GCHQ spooks plotted cyberattacks against telco Belgacom

09/22/2013 23:39 (Computer World Singapore)

...telec providers," the leaked presentation said. This was no mere **spear phishing** expedition; GCHQ got close to accessing the firm's main international...

Gang exploits both physical and system security during bank robbery

09/22/2013 22:02 (Computer World Singapore)

..."demonstrates the rapidly evolving nature of low risk, high financial yield **cyber** enabled **crime**," the law enforcement agency said. "Those responsible...

Building Malaysia's Cyber Security Defense Foundations

09/22/2013 21:43 (Yahoo! Canada Finance)

FBI warns of new malware threat

09/22/2013 19:15 (Galax Gazette)

...Beta Bot: Run a full system scan with up-to-date anti-**virus** software on the infected **computer**. If Beta Bot has blocked access to security sites,

Mobile can help drive more federal innovation

09/22/2013 14:45 (Federal Times)

...reduction in paper processing. Empower employees. When **mobile device** management **security** considerations are coupled with limited available resources,

What The Small Business Owner Needs To Know About Cyber Security

09/21/2013 21:26 (Forbes)

What The Small Business Owner Needs To Know About **Cyber Security** On the topic of **cyber security**, I think that most small business owners file...

Prepare yourself for a nationwide cyber attack

09/21/2013 09:55 (Times Online)

Prepare yourself for a nationwide **cyber attack** Former Homeland **Security** secretary says it s a matter of when not if From the raging fires that...

UK Firms Detect Security Incidents Three Times More Often than Average

09/21/2013 09:27 (Infosecurity)

...them, whereas 28% pinpoint hackers as a source of outsider **security** incidents. As **cyber** threats evolve, it is critical that organizations rethink...

Attack Threat Continues to Increase

09/20/2013 18:29 (Isssource.com)

Attack Threat Continues to Increase **Cyber** threats are continuing to grow and get more sophisticated, a new report said. Cyber threats are continuing...

Eight Busted for Cyber Theft

09/20/2013 17:56 (Isssource.com)

...the rapidly evolving nature of low risk, high financial yield **cyber** enabled **crime**. These arrests were achieved working in partnership with the...

Job Security with Cyber Security

09/20/2013 17:46 (Isssource.com)

Job **Security** with **Cyber Security** There needs to be more **cyber security** professionals to defeat the threats and hacker attacks that are plaguing...

Industry Launches Global Certification Effort Targeting Critical Infrastructure

09/20/2013 15:59 (Infosecurity)

...for industrial control security. The snappily-named Global Industrial **Cyber Security** Professional (GICSP) certification will be developed by a...

Q;A: Attackers target Internet Explorer zero-day flaw

09/20/2013 11:56 (USA Today)

...provide some specifics about how these attacks are taking place? Is it via **phishing**, drive by download, self-replicating script worm? Watson: This...

Barclays Cybercrime Suspects Arrested Over $2.1 Million Theft

09/20/2013 06:07 (Bloomberg)

...a theft potentially worth millions of pounds. Banks face **cyber**-**security** threats from increasingly sophisticated hackers trying to steal customer...

Cash bounty offered to hack Apple's fingerprint sensor

09/20/2013 05:50 (WTSP.com)

...by Nick DePetrillo, @nickdepetrillo, an independent **security** researcher who specializes in finding vulnerabilities in **mobile device** hardware.

Cost of cyber crime study: United States

09/20/2013 02:25 (Help Net Security)

Cost of **cyber crime** study: United States **Cyber** attacks generally refer to criminal activity conducted via the Internet. Cyber attacks generally...

National Guard running drills to protect R.I. from cyberattacks

09/20/2013 01:00 (The Providence Journal (AP))

...shared their methods for deciding whether the anomaly indicated an everyday **computer** glitch or a focused **attack**. The exercises, which started...

Terrorism, cyber crime and budget woes face new FBI director

09/19/2013 23:59 (The Wichita Eagle and Kansas.com)

Terrorism, **cyber crime** and budget woes face new FBI director WASHINGTON Big budget woes worry new FBI Director James Comey, a mere two weeks...

U.S. Energy Department spends $30M to bolster utility cybersecurity tools

09/19/2013 23:03 (Computerworld Malaysia)

...better protect nation's electric grid, oil and gas infrastructure from **cyber**-**attack**. The projects, which will combine power system engineering and...

Hacked: It could happen to you

09/19/2013 22:42 (Computer World Singapore)

...the un-named reseller "unwittingly" responded to a **spear phishing** attack which allowed attackers to access sensitive information, including usernames...

Energy Department spends $30M to bolster utility cybersecurity tools

09/19/2013 19:29 (Knoxville Times)

...better protect nation's electric grid, oil and gas infrastructure from **cyber**-**attack**. The Department of Energy today awarded $30 million to a...

Air Force Research Lab puts money up for tools to stop future Snowdens

09/19/2013 18:00 (Ars Technica)

Air Force Research Lab puts money up for tools to stop future Snowdens AFRL modifies **cyber** research program to find ways to catch "insider threat."

FBI ALERT - Beta Bot malware blocks users anti-virus programs

09/19/2013 12:55 (The Police News)

FBI ALERT - Beta Bot **malware** blocks users anti-virus programs Prepared by the Internet Crime Complaint Center (IC3) Beta Bot **malware** blocks users...

Clicking Through the Cloudy Relationship Between US Feds and Google

09/19/2013 10:19 (Security Today)

...familiar with those letters, ECS is the abbreviation for **Enhanced Cybersecurity Services** a voluntary information sharing program operating from the...

New wave of Shylock Trojan targets bank customers

09/19/2013 07:46 (Help Net Security)

...currently unknown, but the researchers are almost positive that the **malware** is served by an exploit kit that takes advantage of Java vulnerabilities...

NSA wants even closer partnership with tech industry

09/19/2013 05:19 (Computer World Australia)

who gave the keynote address at the New York Institute of Technology **Cyber Security** Conference here, flatly refused to discuss the topic. But...

Latest IE 0-day insight: Background, severity and solutions

09/19/2013 03:52 (Help Net Security)

or it may have been in the private toolkit of the world's best **malware** writers for more than a decade. This is as severe as any browser issue...

ENISA Publishes Mid-Year Summary of Threat Landscape

09/19/2013 08:59 (Infosecurity)

...increasingly become, exploited by cyber-criminals;" that the consumerization of **malware**, exploit kits and services "will open up new avenues for cyber-fraud...

Does DHS Have Too Much Cyber Authority?

09/19/2013 08:52 (GovInfoSecurity)

...About Trust, DHS Responsibilities U.S. citizens understand the role of **government** in maintaining security in the real world, but that's not yet...

Thieves Want Your Identity, Not Your Gadgets

09/19/2013 08:34 (Amazines)

...crack one password, they can get access to everything. Viruses and **Malware** You might be wondering how to prevent identity theft. Be careful what...

Apple iOS 7's New Activation Lock Is Brought To You By Attorney General Eric Schneiderman

09/19/2013 07:00 (The Village Voice Blogs)

...summer, the two offices ordered a "stress test"--inviting **cyber security** experts to try and hack Activation Lock. At the time, Schneiderman and...

Longwood's Cyber Security Center First in Virginia to Receive National Digital Forensics Designation

09/19/2013 06:28 (Digital Journal)

Could Brazil Actually Keep The NSA Out Of Its Internet Traffic?

09/19/2013 06:22 (Mint Press News)

...Agency Network. The ARPANET connected the U.S. Department of **Defense** to the **computer** networks of universities that were working on Defense-funded...

Hacking courses offer cybercrooks tips on how to hone skills

09/19/2013 05:55 (ComputerworldUK.com)

...on helping aspiring hackers learn how to hide their tracks on a **compromised system**, how to evade antivirus and firewall tools and how to use...

Phishers increasingly target brands

09/19/2013 03:25 (Help Net Security)

...increasingly target brands The APWG is reporting in its latest Global **Phishing** Survey: Trends and Domain Name Use study that an increasing number...

Mobile data security remains weak

09/19/2013 02:43 (Help Net Security)

...show that companies are not taking steps to educate employees on **mobile device security** to help protect company data. The increasing popularity...

Pentagon computer network insecure, Gitmo defense counsel says

09/19/2013 00:53 (Stars and Stripes)

Pentagon **computer** network insecure, Gitmo **defense** counsel says GUANTANAMO BAY NAVY BASE, Cuba -- Chronic problems of Pentagon computer network...

"Operation Zombie" Nabs Argentine Hacker

09/18/2013 13:18 (Poker News Daily)

...internet to carry out tasks. In this case, the zombie **computer** had their **security compromised** with malware and directed to implement a DDoS attack...

Will The Next Election Be Hacked?

09/18/2013 10:40 (GlobalResearch.ca)

Most SSL Sites Remain Insecure and Vulnerable

09/18/2013 10:36 (BizTech)

...as a load balancer and that s an additional cost. Lackluster **Digital**-Certificate Management Creates **Security** Gaps It s hard to talk about SSL...

EiQ Networks Survey Reveals What Keeps IT Pros Up at Night

09/18/2013 10:25 (Technology News)

...coupled with increased awareness and implementation of SANS critical **security** controls will help improve **cyber** defenses across organizations."

3 ways malware is bypassing companies' antivirus software

09/18/2013 06:00 (IT Manager Daily)

3 ways **malware** is bypassing companies antivirus software Most companies are using antivirus software, firewalls and other security tools to protect...

Recommendations for strengthening cyber security policies

09/18/2013 05:55 (Help Net Security)

Recommendations for strengthening **cyber security** policies McAfee and the **Digital** Government **Security** Forum (DGSF) released a new report which...

USB "condom" protects from mobile device juice jacking

09/18/2013 03:48 (Help Net Security)

...year's Black Hat conference when they showcased chargers capable of installing **malware** on iPhones, and have brought attention to a type of attack...

Hackers target PDC's network

09/18/2013 03:22 (The Spokesman-Review)

...the public should be assured that the FBI takes seriously **cyber** intrusions that could compromise national **security**. © Copyright 2013 Associated...

You Could Go To Jail For Hacking Your iPhone And Obama Wants To Change That

09/17/2013 19:35 (Yahoo! Canada Finance)

Record number of students to fight off hackers, try to keep computer systems safe

09/17/2013 17:28 (Iowa State University)

...Teams of Iowa State students work to keep hackers out of their **computer** systems during a recent **Cyber Defense** Competition. Teams of Iowa State...

NASDAQ Website Vulnerabilities Went Unpatched for Two Weeks

09/17/2013 17:22 (Infosecurity)

...range of reasons, from simply interfering with websites to launching **phishing** attacks against web users; the scripts can even rewrite the content...

China-based hacking group behind hundreds of attacks on U.S. companies

09/17/2013 15:45 (Computerworld)

The group has a long history of attacking organizations in the **defense industrial base**, financial services sector, education, government, supply...

Microsoft rushes out software fix to prevent browser attacks

09/17/2013 15:32 (Reuters US News)

...about a zero-day bug, other groups of hackers involved in massive **cyber**-**crime** operations, such as identity theft, rush to reverse-engineer the...

Analyst: Pentagon Should Move to Protect 'Core' Industries Before Budgets Collapse

09/17/2013 15:14 (National Defense Magazine - Blog)

...Strategic and Budgetary Assessments. The study, Sustaining the U.S. **Defense Industrial Base** as a Strategic Asset, will be unveiled Sept. 18 on...

Sharing Too Much Information?

09/17/2013 08:50 (GovInfoSecurity)

...multiple white papers and standards, including RFC6545, Real-time Inter-**network Defense**, and is co-chair of the Internet Engineering Task Force's...

Critical Infrastructure Providers Strengthen Cybersecurity by Implementing Standards-Based PKI

09/17/2013 08:28 (Technology News)

...Key Infrastructure (PKI) standards developed by NAESB to strengthen **security** for their **cyber**-based business processes and transactions. Recent...

NSA buys zero-day attack information from French firm, contract shows

09/17/2013 08:27 (GigaOM)

...NSA buys in knowledge of so-called zero-day vulnerabilities that help it **attack computer** systems, a freedom-of-information request in the U.S.

Brazil looks to break from US-centric Internet

09/17/2013 07:25 (HeraldStarOnline.com)

...United States and the European Union in opposition. U.S. **digital security** expert Bruce Schneier says that while Brazil's response is a rational...

Medical Identity Theft Could Cost You Your Life

09/17/2013 07:06 (Amazines)

After Autonomy, Founder Mike Lynch Invests in a Honeypot for Hackers

09/17/2013 06:49 (Bloomberg)

...fund's first investment: Darktrace, which describes itself as a behavioral **cyber defense** platform that seeks to lay bait for hackers -- both those...

Most Hacktivists Just Looking For Attention: Report

09/17/2013 06:41 (Info Packets)

Belgium's largest telecommunications company victim to a nation-state sponsored spying campaign

09/17/2013 04:16 (Live Hacking)

...actually accuse the USA directly. The hack was performed using **malware** with advanced encryption techniques. Belgacom has now removed the unknown...

Most medical identity theft committed by family and friends

09/17/2013 00:00 (DOTmed.com)

Medical identity theft is fast-growing and dangerous

09/16/2013 22:31 (The Dallas Morning News)

FBI arrests local man with ties to hacker group Anonymous

09/16/2013 20:42 (The Monitor (AP))

FBI agents were able to get the internet protocol or IP address of the **computer** used in the **attack**, and they tracked it to a house off Nolana...

Instagram & Identity Theft

09/16/2013 06:59 (Flixya - Blog)

...is essentially all that is needed to begin a full-fledged **phishing** attack. Unfortunately Trend Micro found that users who visit and provide their...

Scambook Warns 4 Million Illinois Healthcare Patients' Social Security Numbers Stolen

09/16/2013 06:54 (Technology News)

...warned of their increased risk of identity theft in the wake of this **computer** theft. Social **Security** numbers, addresses, and dates of birth can...

What CISOs must learn from Bitcoin and a research team at Georgia Tech

09/16/2013 05:24 (Help Net Security)

...are used to analyze the code submitted by the developer). How does **malware** in the app store implicate iOS encryption? Well, the link here is...

Cypersecurity pro on Nasdaq website: 'I needed 10 minutes to hack' - NY Daily News

09/16/2013 02:30 (NY Daily News)

...that hackers could steal users browser history and cookies or perform **phishing** attacks to steal confidential data. But the financial market has...

Bold cyber heist thwarted in London

09/16/2013 02:00 (Seacoast Online (AP))

...very seriously. In their statement, Det. Insp. Mark Raymond described **cyber attack** as a "sophisticated plot that could have led to the loss of...

Week in review: Backdoored NIST standard revealed, Java's new whitelisting feature, and the new issue of (IN)SECURE Magazine

09/16/2013 00:05 (Help Net Security)

...havoc on businesses via DDoS attacks, data breaches and even **malware** or botnet assaults. Security heavyweights to keynote HITB conference in...

The greatest mobile threats (and Android malware isn't one of them)

09/15/2013 20:24 (Computerworld Blogs)

The greatest mobile threats (and Android **malware** isn't one of them) Self-interest is behind a lot of the mobile **malware** reports from anti-virus...

Race is on among tech shops to perfect cyber ID solutions

09/15/2013 15:24 (The News Tribune)

...among tech shops to perfect cyber ID solutions Concerns over privacy, **security** grow as old ways of **digital** verification exposed as risky How does...

Government Standards Agency “Strongly” Suggests Dropping its Own Encryption Standard

09/15/2013 13:25 (Common Dreams)

...Standard Following revelations about the NSA's covert influence on **computer security** standards, the National Institute of Standards and Technology,

Vodafone Germany blames 'insider' after hacker steals 2 million customer records

09/15/2013 08:59 (Computer World Singapore)

...the infamous attack on Sony in 2011. Vodafone has warned of **phishing** attacks using the stolen email addresses, which will be a significant problem...

Cyber security: The new arms race for a new front line

09/15/2013 03:45 (Alaska Dispatch)

...high school talent searches in the form of cybergames like **CyberPatriot**, a hacking tournament pitting young high school students against industry...

WikiLeaks Server Won By Teen Who Bid $33,000 Of His Dad's Money

09/13/2013 17:50 (The Huffington Post)

The hard disks have been erased according to U.S. specification DoD **5220.22**-M where every byte of the hard disk is overwritten several times.

Dropbox takes a peek at files

09/13/2013 05:52 (ComputerworldUK.com)

...wrote. "Are the files being accessed for de-duplication purposes or possibly **malware** scanning? If so, then why are the other file types not being...

Santander Cyber Attack Thwarted by U.K. Police as 12 Arrested

09/13/2013 05:26 (Washington Post - Bloomberg)

Santander **Cyber Attack** Thwarted by U.K. Police as 12 Arrested Sept. 13 (Bloomberg) -- London police arrested 12 men over an attempt to hack into...

Hacker targets millions of German mobile phone customers

09/13/2013 03:45 (Yahoo! News Canada)

Military-grade solution to protect industrial control systems

09/13/2013 01:41 (Help Net Security)

...benefits of increased connectivity while also reducing the risk of **cyber attack** BAE Systems Detica launched IndustrialProtect, a military-grade...

Hack victims urged to share the gory details

09/12/2013 22:27 (Computerworld Malaysia)

Hack victims urged to share the gory details Advanced **Cyber Security** Center in U.S. fosters voluntary information sharing among private organisations...

Massive hack compromises data of two million Vodafone Germany customers

09/12/2013 21:34 (Computerworld Malaysia)

...directly--but it will leave those customers more vulnerable to sophisticated **phishing** scams. The breach only affects Vodafone Germany customers and will...

Google knows nearly every Wi-Fi password in the world

09/12/2013 18:44 (Computerworld Blogs)

...backup data off the wire. And it s great they they have strong **security**, both **digital** and physical, at their data centers. However, Google s...

Kaspersky Lab Analyses Active Cyber-Espionage Campaign Primarily Targeting South Korean Entities

09/12/2013 17:33 (CBS 3 Springfield - WSHM)

...initial delivery mechanism remains unknown, Kaspersky researchers believe the Kimsuky **malware** is most likely delivered via spear-**phishing** e-mails...

Android Malware via Email

09/12/2013 16:45 (Isssource.com)

Android **Malware** via Email A new email spam campaign shows the messages are not spreading drive-by downloads or even peddling ordinary PC **malware**,

Cyber Crime Growing Priority for FBI

09/12/2013 16:21 (Memphis Daily News)

Cyber Crime Growing Priority for FBI Updated 3:06PM Glankler Brown PLLC attorneys on Wednesday, Sept. 11, welcomed FBI Supervisory Special Agent...

Britain's Phone-hacking Scandal Officially Widens to the Sunday Mirror

09/12/2013 15:16 (Infosecurity)

...guardians? The hacking was undertaken with, what else, but **malware**. As AdaptiveMobile s founder and COO Gareth Maclachlan explained at the start...

Hacker steals data of 2mn Vodafone Germany customers

09/12/2013 05:47 (Breitbart News: The Wires)

...name. It warned however of the risk of so-called "**phishing**" attacks in which fake emails try to trick customers into revealing their passwords.

Working on the front lines of cybersecurity

09/12/2013 05:45 (The Wickenburg Sun)

...often debated which sector of our economy is most vulnerable to a **cyber**-**attack** and into which industry a breach would cause greatest disruption.

Research Shows Windows Image Password Too Simple to Crack

09/12/2013 03:28 (EmailWire.com)

...computer as safe as possible with the latest windows internet **security** 2011. Contact Information: **Digital** Delivery Downloads Customer Service...

Guest View: What you should know about advanced persistent threats

09/12/2013 03:13 (Computerworld Malaysia)

Social Engineering: typically, an attacker may create very specific **spear**-**phishing** emails with seemingly harmless attachments that the target will...

NCSA begins research on cyber attack defenses

09/12/2013 01:00 (The Daily Illini)

NCSA begins research on **cyber attack** defenses The University s National Center for Supercomputing Applications has begun research on fortifying...

Cyberspies attack key South Korean institutions, North Korean hackers suspected

09/11/2013 21:58 (Computer World Singapore)

...attackers distribute the Kimsuky Trojan horse program to their targets, but **spear**-**phishing** is a likely possibility, Tarakanov said. The **malware**...

Wis. trucker pleads guilty in Koch cyberattack

09/11/2013 21:03 (TheState.com)

...the hearing. The parties have agreed that the direct loss from the **attack** staged by the **computer** hacking group Anonymous is less than $5,000.

Beware the Hack Attack

09/11/2013 16:23 (Northwest Indiana Business Quarterly Magazine)

...to ensure we are secure as businesses, consumers and individuals? **Phishing** and online scams have been in existence for many years, and things...

The Trojan War: Malware attacks spike, catching NCW users in a hostile web [The Wenatchee World, Wash.]

09/11/2013 15:50 (Technology News)

The Trojan War: **Malware** attacks spike, catching NCW users in a hostile web [The Wenatchee World, Wash.] (Wenatchee World, The (WA) Via Acquire...

10 yrs later, DHS still plagued with cybersecurity, critical infrastructure problems

09/11/2013 13:41 (Computerworld Blogs)

10 yrs later, DHS still plagued with cybersecurity, **critical infrastructure** problems Today marks 12 years after the 9/11 terrorist attacks; it...

North Korean hackers suspected of cyber-espionage attack on South

09/11/2013 12:35 (The Guardian)

...believed to have "infected" the machines using so-called **spear-phishing** emails, which target their victims with personalised messages in the...

Android Malware uses SMTP

09/11/2013 12:28 (Isssource.com)

Android **Malware** uses SMTP A new Android **malware** is using SMTP to send the data it steals to its masters. A new Android **malware** is using SMTP...

Massive Botnet is Behind Tor Usage Spike

09/11/2013 12:06 (Infosecurity)

...one conclusion: somebody out there infected millions of computers [with **malware**] and as part of their plan they installed Tor clients on them,

Crackdown on Cybercriminals Equals Reduced Cybercrime in Russia

09/11/2013 10:30 (Infosecurity)

...internet fraud: down from $697 million to $615 million (with only **phishing**-based fraud bucking the trend and increasing from $55 million to $57...

Android scareware delivered via spoofed email notices

09/11/2013 03:52 (Help Net Security)

...tries to make the victim believe that his phone is infected with a host of **malware**, and offers to clean it up if the user is willing to pay for...

Feds aren't 'knowingly' weakening encryption, says U.S. official

09/11/2013 00:20 (Computerworld Malaysia)

..."is to support a technical understanding of the strongest, most secure **computer security**, including encryption that we can. "We are not deliberately,

Microsoft Patch Tuesday brings critical Explorer, Outlook fixes

09/10/2013 23:40 (Computer World Singapore)

...pointed out that environments with sensitive data could be subject to **spear**-fishing attacks that use these vulnerabilities, in which an attacker...

Cisco takes aim at security services with new division

09/10/2013 23:03 (Computerworld Malaysia)

...providers. Before joining Cisco, Palma was vice president of **Cyber** and **Security** Solutions at Boeing, which sold products and services related...

Email spam campaign distributes Android scareware

09/10/2013 23:03 (Computerworld Malaysia)

...are increasingly looking at email as a method of distributing Android **malware**, researchers say Android **malware** is following in the footsteps of...

New browser blocks snooping adware, Google tracking

09/10/2013 22:47 (Computer World Singapore)

...auto-translate, address bar suggest, spell-check, URL check, **malware** check and home sync. None of a users' browsing traffic passes through Hidden...

Invensys: Information in Context

09/10/2013 19:22 (Isssource.com)

...during the opening session at the conference. We believe safety and **cyber security** will continue to be in demand. With fewer people working in...

Missouri S&T Combats Campus Cyberwoes with Software Donation

09/10/2013 15:16 (Infosecurity)

...computers owned by students, faculty, and staff, against virus, **malware** and other malicious attacks. The products will also be available for research...

Cyber security program recuits in Delaware

09/10/2013 13:41 (NewsWorks)

Cyber security program recuits in Delaware The **Cyber** Aces Foundation is searching for the next class of **cyber security** leaders at local Delaware...

Microsoft Patch Tuesday delivers critical IE, Outlook fixes

09/10/2013 12:24 (Computerworld)

...pointed out that environments with sensitive data could be subject to **spear**-fishing attacks that use these vulnerabilities, in which an attacker...

New gTLD security implications

09/10/2013 11:26 (Help Net Security)

...records, redirecting wayward queries. This opens the door to possible **malware** or **phishing** attacks on unsuspecting systems. However, it s unlikely...

War of the Trojans: 'Alien' Invasion Spreads Third-Party Malware

09/10/2013 10:34 (Infosecurity)

War of the Trojans: 'Alien' Invasion Spreads Third-Party **Malware** A nasty Android trojan, dubbed Obad.a, is being spread using botnets controlled...

9/11 DDoS Alert for Banks, Agencies

09/10/2013 08:20 (GovInfoSecurity)

...University of Alabama at Birmingham who also works for the anti-**phishing** and anti-**malware** firm Malcovery, claims the hacktivist groups' main...

Timing is an influential risk-factor for cyber attacks

09/10/2013 05:46 (Help Net Security)

...wreaking havoc on businesses via DDoS attacks, data breaches and even **malware** or botnet assaults. There are several dates throughout the year that...

Damballa Reports Over 75% of HTTP Malware Evades Detection by Traditional Protection Methods

09/10/2013 01:07 (Technology News)

Damballa Reports Over 75% of HTTP **Malware** Evades Detection by Traditional Protection Methods Sep 10, 2013 (Close-Up Media via COMTEX) -- Damballa,

Android 'Obad' Trojan piggybacks on another gang's mobile botnet

09/09/2013 22:30 (Computer World Singapore)

...in that victim's address book. According to Kaspersky, the **malware** was also being spread via convincing-looking copies of the Google Play store...

Admins work overtime as Microsoft fixes Office with bumper 7 patches

09/09/2013 21:29 (Computerworld Malaysia)

...2011's 100. This was a "good reflection of how challenging the **computer security** business continues to be," he said. The whack taken by Office...

More should be done to implement cyber security strategy in NZ: Netsafe

09/09/2013 17:41 (ComputerWorld)

More should be done to implement **cyber security** strategy in NZ: Netsafe Cost-benefit analysis needs to be a key part of **government** spend on **cyber**...

Auburn named cyber operations center of excellence

09/09/2013 16:51 (Akron Beacon Journal)

Auburn named **cyber** operations center of excellence AUBURN, Ala. AUBURN, Ala.: The National Security Agency has designated Auburn University and...

Is Your Cellphone Private or Not?

09/09/2013 16:39 (DigTriad.com)

...Fourth Amendment questions," says Orin Kerr, an expert on **computer crime** law at George Washington University Law School. "Technology changes...

Botnet Found on Tor

09/09/2013 14:44 (Isssource.com)

...also included Tor connectivity. We have found various references that the **malware** is internally known as SBC to its operators. So, the botnet...

Executives, IT officers most concerned about malicious insiders

09/09/2013 14:44 (Help Net Security)

...professionals, and work for tech and financial firms, telecoms, and the **government** / local authorities. A quarter of the total have said that their organization...

New Way to Spread Android Trojan

09/09/2013 14:13 (Isssource.com)

...variety of data stealing, premium-rate messaging, additional **malware** downloading actions. When they first discovered the Trojan, Kaspersky Lab...

Protecting Domain Names From Hacking Through A Registry Lock

09/09/2013 10:36 (DomainPulse.com)

...password for a US-based [domain name] reseller via a **spear phishing** email closely targeted to the user to fool them into passing the details...

NIST Revising Mobile Forensics Guide

09/09/2013 08:50 (GovInfoSecurity)

...published a draft of Special Publication 800-101 Revision 1: Guidelines on **Mobile Device Forensics**. "In the past, there were enough tools that you...

Fake emails saying US is bombing Syria lead to malware

09/09/2013 08:33 (Help Net Security)

Fake emails saying US is bombing Syria lead to **malware** Two distinct spam campaigns taking advantage of the current political situation in Syria...

McAfee releases 2014 core PC security products

09/09/2013 05:45 (Help Net Security)

...Total Protection 2014. With enhancements to its recently upgraded **malware** scanning engine McAfee AM Core first introduced with the 2013 line,

Anonymous user authentication from LaunchKey

09/09/2013 00:33 (Help Net Security)

...is expected to reach $5.45 billion by 2017. When a **security** breach or **cyber attack** occurs, it can cost companies upwards of hundreds of millions...

Web hacking in Pakistan on the up

09/09/2013 00:32 (Technology News)

hundreds of websites, storing critical and sensitive data concerning national **security**, have been hacked by **cyber** criminals, exposing the gaps...

Week in review: FinFisher's spying capabilities, and NSA's quest to subvert encryption

09/09/2013 00:03 (Help Net Security)

...work as promised RSA researchers have recently spotted a banking **Trojan** targeting Linux systems being sold online by a **cybercrime** team based...

New 'Hesperbot' bank Trojan targets mobile authentication systems

09/08/2013 22:20 (Computerworld Malaysia)

...multi-factor authentication systems rolled out to defeat an older generation of **malware**. Security firm ESET is warning of an ambitious new banking...

Security concerns preventing mobile payments from taking off, report claims

09/08/2013 21:32 (Computer World Singapore)

...benefit from the expected boom in mobile payments, citing concerns around **malware** and fraud. Barclays has led the way in mobile payments in the...

Kaspersky Lab launches Anti-Virus and Internet Security 2014

09/08/2013 12:32 (Computerworld Malaysia)

...advanced Anti-Blocker technologies to deal with the latest developments in **cyber crime**. "We're determined to empower users against the surge...

Android Trojans gain botnet distribution, new code

09/08/2013 12:20 (Computer World Singapore)

...operating system has gained new nefarious capabilities even as a new banking **malware** takes aim at the OS, according to security researchers. A...

Microsoft's picture-authentication welcomed given password fatigue

09/08/2013 11:49 (Computer World Singapore)

...network. In addition, picture passwords can be recorded through **malware** on an infected computer, similar to how a malicious **keylogger** records...

Cyberdefense a big concern in China after NSA reports

09/08/2013 00:36 (The Boston Globe)

...and the ruling Communist Party. But for most people in China, **computer security** is poor, and the damage caused by everyday hacking is immense.

B.C. computer servers linked to global theft ring

09/07/2013 14:21 (Yahoo! News Canada)

How to Avoid the Latest Facebook Scam

09/07/2013 08:18 (Yahoo! Canada Finance)

Mass. cyber security firms untangle Web attacks [Boston Herald]

09/07/2013 07:10 (Technology News)

Mass. **cyber security** firms untangle Web attacks [Boston Herald] (Boston Herald (MA) Via Acquire Media NewsEdge) Sept. 07--A string of high-profile...

Taidoor analysis shows how malware evolves

09/07/2013 07:10 (Infosecurity)

Taidoor analysis shows how **malware** evolves Real world viruses adapt over time in order to survive against antibiotics. Cyber viruses and trojans...

MSU Among Top Cyber Educators

09/07/2013 06:16 (Technology News)

MSU Among Top **Cyber** Educators (Targeted News Service Via Acquire Media NewsEdge) STARKVILLE, Miss. (Targeted News Service Via Acquire Media NewsEdge)

In any US-Syria conflict, cyberweapons could fly in both directions

09/06/2013 20:36 (Yahoo! News Canada)

Patch Tuesday Preview: September 2013

09/06/2013 04:51 (Infosecurity)

...problem: "Network administrators will likely see an uptick in **phishing** attacks using crafted Office documents as attackers quickly reverse Microsoft...

US carried out 231 'cyber-operations' in 2011 alone, leaked documents show

09/06/2013 00:49 (Computerworld Malaysia)

...confirmed. The US is known beyond reasonable doubt to have launched the **Stuxnet** attacks on Iran's Natanz nuclear enrichment plant going back as far...

Samsung fortifies enterprise security on its Android phones

09/05/2013 21:59 (Computerworld Malaysia)

...the Android ecosystem. "It will open up a conversation around **security** at the **mobile device** that will allow for broader adoption of BYOD devices...

Linux 'Hand of Thief ' bank Trojan is not viable malware, says RSA

09/05/2013 21:59 (Computerworld Malaysia)

Linux 'Hand of Thief ' bank Trojan is not viable **malware**, says RSA Protoype's capabilities oversold The 'Hand of Thief' (HoT) Linux banking Trojan...

NIST Cyber Security Framework proposal provides no 'measurable cybersecurity assurance'

09/05/2013 21:25 (Computer World Singapore)

NIST **Cyber Security** Framework proposal provides no 'measurable cybersecurity assurance' The latest draft of the **Cyber Security** Framework (CSF)

Sandboxing Fail: 75% of Malware Can Still Sneak Past IPS

09/05/2013 17:32 (Infosecurity)

Sandboxing Fail: 75% of **Malware** Can Still Sneak Past IPS Even though the next generation of **malware** is starting to take advantage of non-HTTP...

NSA Adds 4 More Cyber Schools

09/05/2013 17:30 (Isssource.com)

NSA Adds 4 More **Cyber** Schools In a move to cultivate more U.S. **cyber** professionals in the fast moving global security environment, the National...

IT Report: Security Still Lacking

09/05/2013 16:29 (Isssource.com)

...sufficient investment in IT security, and only 34 percent of **government** and defense organizations said they have enough time and resources to...

Microsoft to patch dangerous Outlook hack-by-preview bug next week

09/05/2013 15:25 (ComputerworldUK.com)

...by Gregg Keizer on Computerworld.com. Read more about **malware** and vulnerabilities in Computerworld's **Malware** and Vulnerabilities Topic Center.

Weathering the financial fallout of a data breach

09/05/2013 12:57 (SecurityInfoWatch.com)

...can be sizeable. In a 2013 study by the Ponemon Institute, "Managing **Cyber Security** as a Business Risk: **Cyber** Insurance in the Digital Age," 56...

Comment: Cybercrime Goes Back to the Future

09/05/2013 12:25 (Infosecurity)

...signatures. In the era of the advanced persistent threats (APT), **malware** attacks are a lot more subtle, intelligent, but much more dangerous.

Hand of Thief Trojan Has No Claws

09/05/2013 11:56 (Infosecurity)

Hand of Thief **Trojan** Has No Claws The Hand of Thief (HoT) **trojan** made waves when it hit the Russian **cybercrime** underground in July, claiming...

Damballa Finds over 75% of HTTP Malware Evades Detection by Traditional Protection Methods

09/05/2013 10:09 (Technology News)

Damballa Finds over 75% of HTTP **Malware** Evades Detection by Traditional Protection Methods ATLANTA --(Business Wire)-- Damballa, the advanced...

'Cyber Aces' identifies skills in emerging field

09/05/2013 06:37 (TheState.com)

...to help people identify whether they're skilled in the emerging field of **cyber**-**security**. The "**Cyber** Aces State Championship" is gearing up for...

New advanced banking Trojan in the wild

09/05/2013 04:54 (Help Net Security)

New advanced banking Trojan in the wild ESET **malware** researchers have uncovered a new and effective banking Trojan which targets online banking...

US may launch cyber attacks on Syria: Experts

09/05/2013 03:20 (Albuquerque Express)

...weapons use, American experts said. Cyber experts believe the **government** could use computer viruses to destroy Syrian defences and equipment and...

61% of IT pros don't report security risks to executives

09/05/2013 02:16 (Help Net Security)

...common language that enables the a broader business conversation about **cyber security** risks, particularly when dealing with non-technical executives...

Security Response: Targeted attacks deliver disassembled malware

09/05/2013 00:40 (Computer World Singapore)

Security Response: Targeted attacks deliver disassembled **malware** Shortcut files are fast becoming a common vehicle used in targeted attacks to...

Hacked at it again: Cyber insecurity and news media

09/05/2013 00:21 (The State Press)

hours. It is believed that the Syrian Electronic Army carried out the **cyber attack**. The website was also attacked earlier this year by suspected Chinese...

How registrar locks can stop spear phishing

09/04/2013 21:08 (USA Today)

How registrar locks can stop **spear phishing** SHARECONNECTTWEETCOMMENTEMAILMORE SEATTLE -- Bruce Tonkin, Chief Technology Officer at Melbourne...

A Moveable RAT

09/04/2013 20:02 (Isssource.com)

...present on a compromised machine and whether there is enough memory for the **malware**. If so, it then creates a hidden My Pictures directory that...

Patched Safari Bug under Attack

09/04/2013 18:01 (Isssource.com)

...of known and patched vulnerabilities see more use by cybercriminals and **malware** and exploit kit creators far more than Zero Days. Such attacks...

APT malware NetTraveler learning new tricks

09/04/2013 13:26 (Computerworld Malaysia)

...training their sights on Java. In one flavor of the attack, **spear phishing** messages containing malicious links are sent to likely targets. The link...

Botnet Keeps Morphing, Growing

09/04/2013 10:55 (Isssource.com)

...blacklist of IP addresses known to be participating in spreading spam or **malware**. Personally, I haven t seen anything ever use a composite blocking...

State-Sponsored Cyber Attacks: We Ain't Seen Nothing Yet

09/04/2013 10:33 (Technology News)

...when North Korea announced it has built an army of 3,000 **cyber** trolls to **attack** South Korean websites. Philip Lieberman, President and CEO of...

Why Industry is Losing the Battle Against State-Sponsored Attacks

09/04/2013 10:03 (Infosecurity)

...against the South. This week, sales literature for the FinFisher **government** spyware was leaked onto the internet. This is just one of several...

Fake Facebook "Pages you might like" emails deliver malware

09/04/2013 09:26 (Help Net Security)

Fake Facebook "Pages you might like" emails deliver **malware** Fake Facebook emails urging users to review some Pages they might like are hitting...

Hackers find paths into car computers

09/04/2013 05:17 (The Tennessean)

...system. To be sure, the hackers involved were well-intentioned **computer security** experts, and it took both groups months to break into the computers.

Phishing at root of elaborate cyberattacks

09/04/2013 05:02 (First Coast News)

...used to target individuals to receive an e-mail ruse known as a **spear phishing** attack. The e-mail carries a viral PDF attachment or Web link.

Head of INTERPOL on the key to protecting cyberspace

09/04/2013 02:43 (Help Net Security)

...2014. A key objective of the IGCI is to bring together **digital security** experts from law enforcement, academia and the private sector to work...

US likely to wage cyber attacks against Syria

09/04/2013 01:45 (The Hill - Blog)

...vulnerable to more destructive cyberattacks. Finan argued that the **government** should think more creatively about its cyber strategy. He said...

Mobile Spam Risks on Rise

09/03/2013 22:09 (Isssource.com)

...so much screen real estate so it s harder to tell what is a **phishing** message or something genuine. Cook also said the high-end capabilities of...

Beware of the Pitfalls of Public Wi-Fi

09/03/2013 18:35 (The Afro News)

Hackers can Forge Java Security

09/03/2013 18:33 (Isssource.com)

...warns users if they are about to execute an app not signed with a **digital** certificate, but a **security** expert found it is easy to forge the name...

Computer scam resurfaces and targets South Dakota consumers

09/03/2013 15:18 (Vermillion Plain Talk)

...received a telephone call from someone posing as a well-known **computer** company. These fake **security** experts claim that the computers are at risk...

Android 4.4 to be officially called KitKat

09/03/2013 15:11 (ComputerworldUK.com)

...he recognized there might be risks if Android 4.4 is vulnerable to **malware**. The name was kept secret for the past nine months so it would come...

Why keeping the Internet safe is a shared responsibility

09/03/2013 14:47 (The Daily Journal (AP))

...also practical. For example, AMD joined with Honeywell, Intel, **Lockheed Martin** and RSA to co-found the **Cyber Security** Research Alliance (CSRA),

Hand of Thief Linux Trojan fails to work as promised

09/03/2013 14:45 (Help Net Security)

...work as promised RSA researchers have recently spotted a banking **Trojan** targeting Linux systems being sold online by a **cybercrime** team based...

'New York Times' hack exposes Internet's weaknesses [Global Data Point]

09/03/2013 12:04 (Technology News)

...time. Their copies took hours to be updated with the fix. **Computer security** experts warned that as these attacks grow more common, Internet users...

Phishers cast a wide net and catch a whale: The New York Times

09/02/2013 22:47 (Computerworld Malaysia)

...got fooled by one of the oldest tricks in the book. The **phishing** email. The attack allegedly carried out by the Syrian Electronic Army started...

Even suspicious email is too tempting to skip, survey finds

09/02/2013 22:19 (Computer World Singapore)

...means. But of those surveyed, one in 11 admitted to having **infected** their **system** after they opened a malicious email attachment. Given the fact...

New York Times attack demonstrates power of phishing, hacktivism: Websense

09/02/2013 21:59 (Computer World Singapore)

New York Times attack demonstrates power of **phishing**, hacktivism: Websense The volatile nature of the Internet was demonstrated once again last...

Windows XP's user share nose-dives

09/02/2013 21:57 (Computer World Singapore)

...security group warned that the aged OS will become a prime target for **cyber** criminals once **security** updates end on April 8, 2014. But those calls...

How Apple is improving mobile app security

09/02/2013 21:57 (Computer World Singapore)

...App Store, all apps are manually reviewed by Apple for flaws and **malware**. The large number of submissions, combined with the need to approve...

The fanciful world of cyber warfare

09/02/2013 19:29 (The Guardian)

The fanciful world of **cyber** warfare The explosion was catastrophic. The explosion was catastrophic. When the gas pipeline ruptured that day in...

Marine website compromised with pro-Assad message

09/02/2013 16:58 (KOMO News)

...sophisticated technology methods," said Howard Schmidt, a former Obama **cyber security** advisor. The hackers sometimes throw a bunch of thumb drivers...

The TAO of NSA

09/02/2013 12:41 (Help Net Security)

...(reportedly) 600 people strong TAO might be the unit that generated **Stuxnet** and Flame, but the NSA does not rely only on these operatives to...

Tor is Not as Safe as You May Think

09/02/2013 12:03 (Infosecurity)

...A new research paper, due to be presented at the 20th ACM **Computer** and Communications **Security** Conference (CCS 2013) at Berlin in November, has...

Government employees feel cyber security is important

09/02/2013 06:30 (Help Net Security)

Government employees feel **cyber security** is important Despite high awareness in the public sector about **cyber-security** risks and the threat to...

BLOG: Virtualisation and cloud – What to fear and what to embrace?

09/02/2013 03:07 (Computer World Singapore)

...quickly as virtualisation has. IT security threats and **malware** in particular have become increasingly adept at avoiding traditional signatures.

Apps and file sharing services have changed the security landscape: Check Point

09/01/2013 21:50 (Computerworld Malaysia)

you're opening a back door to the network, letting people put **malware** on your computer and take data from the organisation." The virtual sandbox...

What is the Syrian Electronic Army?

09/01/2013 09:06 (Yahoo! News Canada)

Cyber attack threat: U.S. beefs up security measures before possible military strike on Syria

09/01/2013 06:38 (WPTV NewsChannel 5)

Cyber attack threat: U.S. beefs up security measures before possible military strike on Syria FBI warns of a higher risk of cyber attacks (CNN)

CDM Thanks Our Sponsor:

THE BEST DEFENSE IS OUR DEFENSE

With AppRiver, you can build layers of protection against hackers, spammers, scammers and online crooks. AppRiver's services are easy, effective and affordable. Plus, all of them come with a 30-day free trial and 24/ US-based Phenomenal Care.

Spam & Virus Protection • Web Security • Email Encryption • Secure Exchange Hosting

appriver®
Email & Web Security Experts™

www.appriver.com
sales@appriver.com
(866) 223-4645

Top Twenty INFOSEC Open Sources

Our Editor Picks His Favorite Open Sources You Can Put to Work Today

There are so many projects at sourceforge it's hard to keep up with them. However, that's not where we are going to find our growing list of the top twenty infosec open sources. Some of them have been around for a long time and continue to evolve, others are fairly new. These are the Editor favorites that you can use at work and some at home to increase your security posture, reduce your risk and harden your systems. While there are many great free tools out there, these are open sources which means they comply with a GPL license of some sort that you should read and feel comfortable with before deploying. For example, typically, if you improve the code in any of these open sources, you are required to share your tweaks with the entire community – nothing proprietary here.

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network Protocol Analyser
6. Metasploit.org – The Best Suite for Penetration Testing and Exploitation
7. OpenCA.org – The Leading Open Source Certificate and PKI Management
8. Stunnel.org – The First Open Source SSL VPN Tunneling Project
9. NetFilter.org – The First Open Source Firewall Based Upon IPTables
10. ClamAV – The Industry Standard Open Source Antivirus Scanner
11. PFSense.org – The Very Powerful Open Source Firewall and Router
12. OSSIM – Open Source Security Information Event Management (SIEM)
13. OpenSwan.org – The Open Source IPSEC VPN for Linux
14. DansGuardian.org – The Award Winning Open Source Content Filter
15. OSSTMM.org – Open Source Security Test Methodology
16. CVE.MITRE.org – The World's Most Open Vulnerability Definitions
17. OVAL.MITRE.org – The World's Standard for Host-based Vulnerabilities
18. WiKiD Community Edition – The Best Open Two Factor Authentication
19. Suricata – Next Generation Open Source IDS/IPS Technology
20. CryptoCat – The Open Source Encrypted Instant Messaging Platform

Please do enjoy and share your comments with us – if you know of others you think should make our list of the Top Twenty Open Sources for Information Security, do let us know at marketing@cyberdefensemagazine.com.

(Source: CDM)

National Information Security Group Offers FREE Techtips

Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

The best service of NAISG are their free Techtips. It works like this, you join the Techtips mailing list.

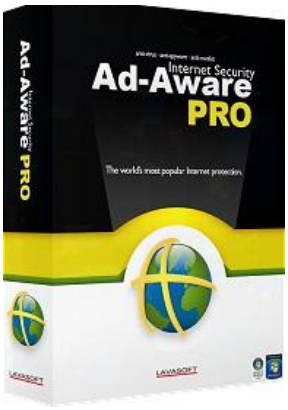
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting your question to the Techtips newsgroup.

Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

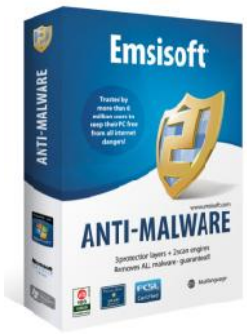
http://www.naisg.org/techtips.asp

SOURCES: CDM and NAISG.ORG



SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com



where they (like you) will be entered into a monthly drawing for the Award winning Lavasoft Ad-Aware Pro, Emsisoft Anti-malware and our new favorite system 'cleaner' from East-Tec called Eraser 2013.

Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Warnings e-Magazines will also keep you up to speed on what's happening in the cyber crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy.

You get all of this for FREE, always, for our electronic editions.

Click here to signup today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

Cyber Defense Magazine - Cyber Warnings rev. date: 09/30/2013

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine July 2013

Sample Sponsors:

To learn more about us, visit us online at http://www.cyberdefensemagazine.com/

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

SAVE $700
BY NOVEMBER 15

Get More in 2014

Elevate your status within your industry. Share ideas with other experts in your field and build your professional network

Gain skills you can actually use on the job. 1 NEW track: Analytics and Forensics, plus MORE tutorials

Access the latest security technology. Explore our BIGGER Expo with 350+ companies

2 Expos
350+ Innovative Exhibitors
280+ Informative Sessions
21 Essential Tracks
5 Days of learning and discovery
1 Premier information security event

FOLLOW US ON: #RSAC

Register Now! www.rsaconference.com/cyberdefense

Global Diamond Sponsors: JUNIPER NETWORKS, Microsoft, RSA

Global Platinum Sponsors: cisco, FireEye

Global Gold Sponsors: Akamai FASTER FORWARD, ixia, splunk>

Platinum Sponsors: hp, McAfee An Intel Company, QUALYS, Symantec

Gold Sponsors: HOB, SOPHOS, IT Security Made in Germany, TREND MICRO, websense