CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

BLACK HAT SPECIAL EDITION

JULY 2013

INSIDER THREATS

MOBILE ATTACK WAVE

BYOD AND MORE...

black hat® USA 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
Tim Pierson
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

Black Hat 2013: USA Has Finally Arrived!

Perfectly timed to followup our last month's edition about Surveillance, In a rare public appearance amid the ongoing US surveillance controversy, the director of the National Security Agency is scheduled to speak to a conference of hackers in Las Vegas later this month. Army General Keith Alexander, the director of the NSA and the leader of the US Cyber Command, is slated to give a keynote presentation at Black Hat, a convention that bills itself as bringing together "all facets of the infosec [information security] world – from the corporate and government sectors to academic and even underground researchers." Alexander has been confirmed to address Black Hat since mid-May, before the Guardian and the Washington Post, relying on leaks from ex-NSA contractor Edward Snowden, revealed widespread NSA surveillance on Americans' phone records and the online habits of persons the NSA believes to be non-Americans living outside the US. "We are honored to have General Alexander join us this year at Black Hat in Las Vegas for the first time. We couldn't have asked for a better time to welcome him," said Black Hat general manager Trey Ford. "The security and intelligence communities have common interest in protecting international critical infrastructure and the internet at large. We both have an acute interest in defining and defending privacy." As befits one of the US's spymasters, Alexander rarely speaks publicly, and his public appearances beyond the Beltway are rarer still. The last time Alexander did so, he sparked a controversy that got his nominal boss, director of National Intelligence James Clapper, in serious trouble. Last year, Alexander addressed a different Las Vegas hacker conference, Def Con, and stated in response to an audience question that "the story that we have millions or hundreds of millions of dossiers on people is absolutely false". The conference's representatives say Alexander is due to speak at 9am on July 31.

We at Cyber Defense Magazine, look forward to sharing more information this once with you about Black Hat 2013 USA Conference along with some excellent articles on Insider Threats, the New Wave of Mobile Malware, the Risks of Bring Your Own Device (BYOD) and so much more.

Pierluigi Paganini

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

P.S. Congrats to Delf Centeno of Guam (USA) – this month's contest winner!

Welcome to Black Hat 2013: USA – Las Vegas, Nevada

We're pleased that Cyber Defense Magazine is now a Media Sponsor of this amazing InfoSec gathering. This is one of the biggest hacker gatherings in the USA, this year taking place at the Caesar's Palace.

The keynote speaker lineup and agenda is pretty amazing and there will be a mix of hackers and Federal agents in attendance although DEF CON is asking the Feds to stay away this year.

The Black Hat conference and DEF CON are where you will find hats of all shapes, sizes and colors – from white hats to grey hats to black hats, all wanting to 'mind meld' and exchange new and exciting ways to break into systems, sharing critical vulnerability research as well as harden systems, along with new forms of malware and attack vectors moving from mobile smartphones to mobile vehicles – yes CAR hacking is on topic and the list goes on.

On a bittersweet note, Barnaby Jack, a celebrated computer hacker who forced bank ATMs to spit out cash and sparked safety improvements in medical devices, died in San Francisco, a week before he was due to make a high-profile presentation at a hacking conference. The New Zealand-born Jack, 35, was found dead, one late Thursday evening in June, 2013, by "a loved one" at an apartment in San Francisco's Nob Hill neighborhood, according to a police spokesman. He would not say what caused Jack's death but said police had ruled out foul play. (Source: Reuters).

There's just so much going on this week from July 27 – August 1, 2013 that we've decided to point you in the right directly quickly, where you can sort through the entire event schedule and much more.

Just click on the magic "black hat" and our little friendly bunny will whisk you away and over to this event, online:

If you have the opportunity to attend, you won't be disappointed. With Snowden on the run and the NSA spying being such a major topic, it's going to be an interesting week, to say the least.

(Source: Cyber Defense Magazine)

PWNIE EXPRESS

black hat USA 2013

#1

7.31

Caesar's Palace - Milano Room 1

DEFCON

#19

8.1 - 8.4

Rio Grande Hotel - Las Vegas

PWNIE PRESENTS:

DEFCON WIRELESS VILLAGE:
Wireless Pentesting with the Pwn Pad

Join the Pwnie Express team for a demonstration of the Pwn Pad in action. Attendees will gain knowledge of and access to plug & play tools that allow you to test for wireless vulnerabilities, enable visualization of the wireless spectrum, and shine a light on wireless client vulnerabilities. The session will start with an overview of wireless security and dive into a practical demonstration of how to test for known vulnerabilities.

BLACKHAT:
How to Pentest 1,000 Branch Offices

CTO Jonathan Cran will demonstrate techniques and tools for penetration testing across an enterprise. Building on the foundation provided by Pwnie Express products, and focusing specifically on high value targets, Jonathan will demonstrate methods for scaling your current testing procedures.

PwnieExpress.com

From Compromise to Detection - The Challenges of Cyber Analytics

By Lee Vorthman Manager, Cyber Initiatives NetApp U.S. Public Sector

In my last article about The Challenges of Near Real-Time Situational Awareness I highlighted several key challenges that need to be addressed to achieve cyber situational awareness. One of the biggest issues I highlighted is the challenge of cyber analytics, which mimics a big data problem. The volume of data combined with the increasing sophistication of attacks mean that compromises can go unnoticed for months or even years before they are detected. Recent statistics from the 2013 Verizon Data Breach Investigation Report indicate that 66% of compromises take months *or longer* to discover. The two most prevalent forms of detection rely on either signatures or statistical analysis. However, both have their weaknesses, and based on the constant news headlines about cyber attacks, clearly aren't catching everything. Given this stark reality, the following questions remain: How can we improve the detection ability of the current cyber analytics tools and how close to real-time situational awareness can we get?

The problem faced by security analysts is similar to the problem faced by astrophysicists who want to detect a distant star, or by missile defense systems that need to shoot down an incoming missile – how quickly and accurately can we detect a signal among noise? Signal detection theory gives us rough guidelines – we can set our detection criteria in a way that will give us the desired ratio of type one and type two errors and we can decrease the amount of noise by increasing the quality of the signal. In cyber analytics neither of these problems are trivial. The fact of the matter is that most attacks like RATs, APTs and other malware use common traffic vectors (http, https, dns) and therefore appear as normal traffic.

Given this difficulty in detecting compromises, it is apparent that any delay in real-time situational awareness is due to the time difference between compromise and detection. Decreasing this detection gap requires powerful analytics that can quickly process large volumes of data and will ultimately improve the ability to detect these events. Current perimeter devices, such as intrusion detection systems, don't have the required processing power. To overcome this limitation, the current trend in cyber analytics is to

deploy a separate technology like Hadoop for cyber analytics, but the batch processing nature of Hadoop makes it better suited for post-analysis than for real-time analytics. Newer analytics platforms like Storm (http://storm-project.net) offer real-time distributed analytics that can begin to address the volume, complexity and real-time requirements of cyber analytics.

With new analytics technologies, security analysts will need to modify their approach in order to achieve near real-time situational awareness. First, analysts need to work closely with their security operations center and traditional IT to collect information from both traditional and non-traditional sources. Once these data sources are being collected, analysts can begin to ask "what is normal?" by effectively establishing a noise floor. Second, numerous sources of data will allow the analysts to tune their analytics platform by correlating results with other data. For example, is it normal for a system to beacon to a remote website? Perhaps it is an indicator of compromise (IOC) or perhaps it is a routine update. Tuning the system will result in faster and more accurate detection of compromises. Lastly, as the technology of cyber analytics progresses we will be able to abstract the human element from the analytics process. This means we will have a greater amount of automation and, ultimately, faster results.

Given the current interest in cybersecurity I am excited about what the future holds for cyber analytics. Combining real-time distributed analytics with increased processing power and flash storage means we will be able to collect and process the volumes of data necessary for real-time cyber analytics. These advances in technology will also enable the application of analytic techniques from other industries such as astrophysics and genetic engineering that will make detection even faster and more accurate. Ultimately, the Holy Grail for security analysts is to detect and block an attack in progress. However, for now I will settle for decreasing the Verizon statistic for average detection of compromises from months to hours!

Lee Vorthman runs cyber defense programs for NetApp's US. Public Sector Division, located in Vienna, Virginia.

Lee can be reached online at lee.vorthman@netapp.com and at our company website www.netapp.com.

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

Time Sensitive InfoSec Innovators Marketplace Opportunities

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

Now Includes:

Your Graphic or Logo

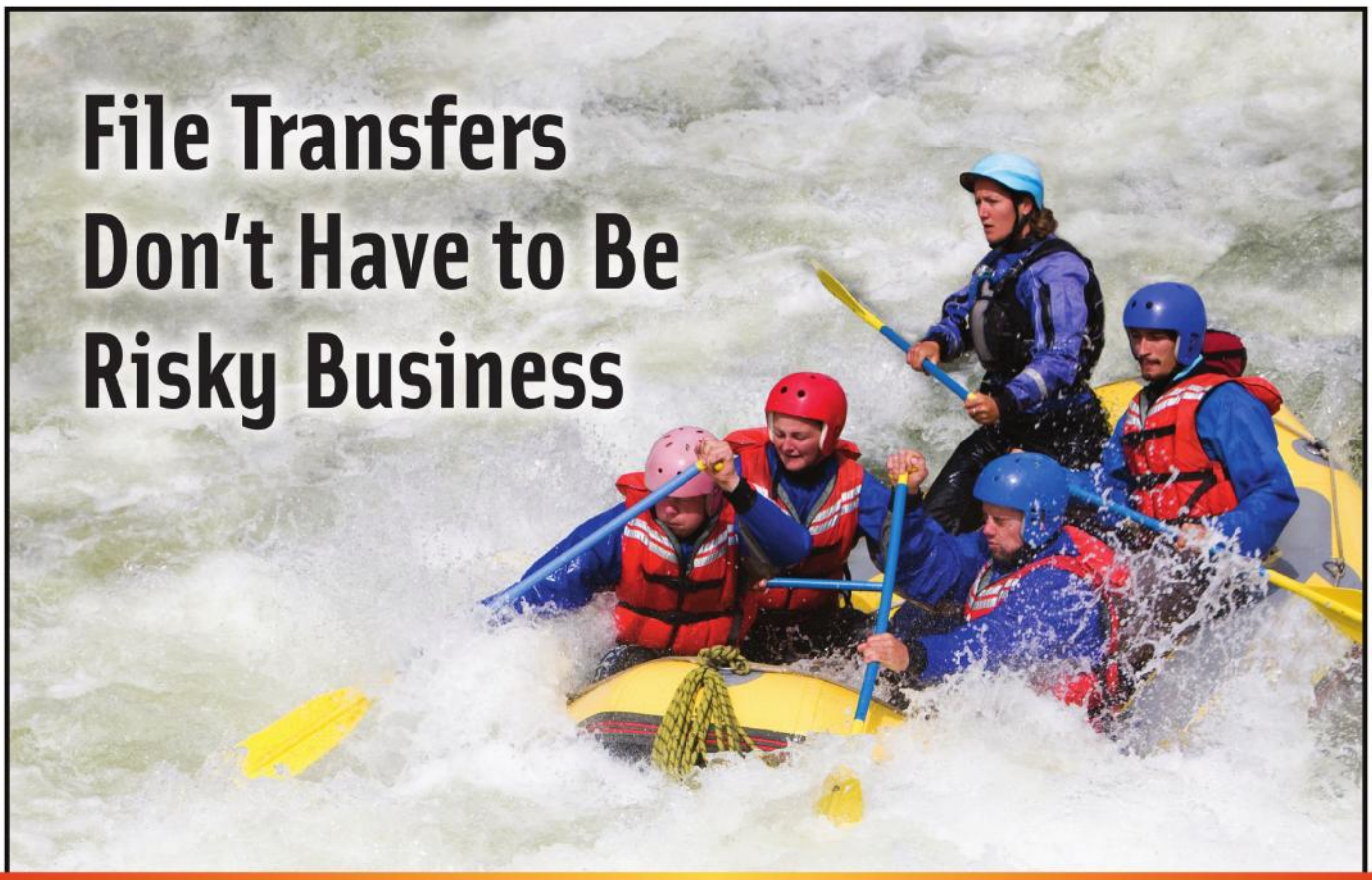
Page-over Popup with More Information

Hyperlink to your website

http://www.cyberdefensemagazine.com/infosec-innovators-marketplace

If you are interested in this unique opportunity or would like to receive a media kit, please contact Jessica Quinn – jessicaq@cyberdefensemagazine.com or toll free in the USA 1-800-518-5248 x2002, International: +1-603-421-6832

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.**

> **"GoAnywhere is flexible enough to let us deliver the files using whatever transfer and encryption method is required."**
>
> *Evelyn Aldis, Adams County Government, Colorado*

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

Will Science and Technology Combine to Eliminate Insider Threats?

Cybersecurity has gained an unprecedented amount of attention in the last decade. Traditionally, threats involve nation state hacking, cybercrime, hacktivism, and malware. However, an increasing number of insider threat incidents, which pose potentially greater ramifications to both public and private networks, are also causing significant damage.

The cyber insider threat is not based on unauthorized access by unauthorized individuals, but rather, by authorized access authorized individuals. Insider threats are currently the number one security problem facing most organizations.. According to a study by the US Secret Service and US Computer Emergency Readiness Team (CERT), a staggering 83 percent of insider threat cases involve attacks that took place from within the insider's physical offices-- in 70 percent of the cases, the incidents took place during normal business hours. Insider attacks are also far more costly to companies than external breaches.

Perhaps the most insidious aspect of insider threats is that the majority of these attacks go unreported. According to the 2011 Cybersecurity Watch Survey, almost 72 percent of insider incidents are handled internally without legal action or the involvement of law enforcement. In most instances, this is because there is a lack of evidence to prosecute, an inability to identify the perpetrator, or fear of public embarrassment.

Nevertheless, some notable incidents warrant discussion.

- On August 29, 2012, a software engineer at Motorola, Hanjuan Jin, was sentenced to four years' imprisonment for stealing Motorola trade secrets. Jin had been at Motorola from 1998 through February 2007, and while on medical leave in 2006, Jin accepted employment with a Chinese competitor company, Sun Kaisens. Once Jin returned to Motorola in February 2007, she downloaded from Motorola's secure internal computer network, numerous proprietary technical documents and removed several documents and other materials from the company's offices. Soon after these activities, on February 27, 2007, Jin gave notice to Motorola that she would be leaving the company. The following day, she was arrested at Chicago's O'Hare Airport after purchasing a one-way ticket to China.

- In February 2010, Greg Chung, a former Rockwell and Boeing engineer, was sentenced to more than 15 years' imprisonment for acting as an agent of the People's Republic of China (PRC) and stealing trade secrets about the Space Shuttle, the Delta IV rocket, and the C-17 military cargo jet for the benefit of the Chinese government.

- In December 2012, Switzerland's intelligence service (the NDB) informed their US and British counterparts of a major data theft by a disgruntled NDB IT administrator involving terabytes of sensitive and classified data.

- And, of course, most recently, Edward Snowden, a former National Security Agency (NSA) employee, leaked details of classified American and British government mass surveillance programs to news corporations, handing over top secret documents he had downloaded from government networks. On June 14, 2013, US federal prosecuters filed a complaint charging Snowden with theft of government property, unauthorized communications of national defense information, and willful communication of classified intelligence to an unauthorized person.

Ironically, despite the damage that can be done, most companies and government agencies prefer not to address the issue with a single solution, but are usually address each incident on a case-by-case basis. This means that the market for a solution, even if found, might be limited--a sure way to prevent R&D investment. Given that the malicious insider already has access to the network, in order to stop their activity a solution must attempt to detect the insider's intent, capability, or mission. And that's a problem today's technology is not able to solve. Behavioral analysis, however, could do the trick.

According to the 2012 Cyber Security Watch Survey half of the internal perpetrators displayed characteristics that indicated they might violate IT security policies prior to committing a cyber crime. And that includes current or former employees, contractors, or other business partners who all have or had authorized access to the network, systems, and/or data. Interesting.

Clearly, being able to identify this behavior would be a major step toward solving the problem. A product designed specifically to leveraging predictive analytics and artificial intelligence capabilities could seamlessly integrate within existing IT appliances, networks and infrastructure to monitor and detect insider threat activities. Through the use of mathematics and algorithms specifically developed to learn the signature of innumerable malicious activities, a solution to protect both public and private networks, safeguarding vital information from insider attacks could be groundbreaking. It's possible, and it's possible today.

Using a combination of big data, predictive analytics and neural networks can result in a product that successfully reports on anomalous or threat indicative employee behaviors and subsequently alerts SOC personnel in near real time. Seemingly unrelated events can be recorded and then correlated to report those employees whose activities fall outside the norm. And the two elements that would make up this solution are already in the marketplace.

First, an enormous amount of data would be necessary to come to the right behavioral conclusions. There are a few corporate entities that have begun working in this area and all use their own proprietary means of finding critical, useful data points among seemingly infinite data streams. Innovators such as the scientists and mathematicians at SQRRL, for example, have come up with the means and technology to store and parse gigantic amounts of data while simultaneously securing that data. SQRRL has modified the Accumulo system to meet their clients' needs for intelligently and securely mining all manner of data for a wide variety of missions in real time. Other groups like PacketSled have developed new methods of mining packetized data by ignoring the packet itself. Instead, they focus their data mining skills on the metadata of the packet, thus optimizing their potential for storage, speed and accuracy necessary to find critical data points.

The second component must provide analytical insight—something that has become one of the most important topics for CISOs and CSOs. In fact,according to a Gartner study, in 2012 the "need for predictive and better security analytics will be the next golden goose for the foreseeable future."

Traditionally, analysts in retail, manufacturing and many other industries have used a variety of statistical methods to solve a range of problems in forecasting, data classification and pattern recognition. Newly developed neural networks, however, can replace all of these methods and produce more accurate forecasts, requiring fewer statistical assumptions while managing complex predictive analytics tasks in a more automated way.

So, just what is a neural network?

They have been designed to mimic how the brain learns and analyzes information. Essentially, a computer based neural network is created in similar ways to a human nerve synapse. Once created, the integration of algorithms and technical input allows the synapses present in the artificial neural network to learn; to process data just as a quickly and intelligently as a human brain. Once trained to learn, a neural network is much more efficient and accurate in circumstances where complex predictive analytics is required. This is because, just like our brains, neural networks are composed of a series of interconnected calculating nodes that are designed to map a set of inputs into one or more output signals. Neural networks can also adapt to changes in a fluid data series and can produce reliable forecasts even when the data series contains a good deal of noise or when only a short series is available for training. These networks are also used extensively in statistical pattern recognition. These include natural language processing, speech and text recognition, and facial recognition. In cyber security, organizations are beginning to research how to harness the power of these neural networks to combat cyber threats by leveraging their ability to identify behavior specifically linked to cyber threat data. The results are exponentially decreasing false positive rates and vastly improved detection for external threats. if this is true for external threats, then why not internal?

There is no question that in the next few years a single solution will be developed. Work is already underway. It will leverage all of these different technical innovations and systematically combine them to build an unique product to monitor employee behavior and begin early detection of the insider threat. The use of massive data storage and secure parsing capacity such as that offered by SQRRL combined with the power of pattern recognition and analytical capacity offered by neural networks will seek out golden data points within the mass of security and network traffic that is already present on corporate networks. The combination of this biologic approach with follow-on analytic tools such as those offered by like PacketSled, Promia, and Bit9, could create a comprehensive network management and security suite of near perfection. I can assure you that work has already begun.

Here is another interesting point regarding the ease or difficulty of detecting an insider threat before it happens. A 2012 study by Carnegie Mellon University's Software Engineering Institute, which evaluated fraud and illicit cyber activity in the US financial services sector, produced intriguing results. The study concluded that while an average of 32 months elapsed between the beginning of a fraud and its detection by the victim organization, the insiders' means were not especially sophisticated. It doesn't mean the perpetrators are stupid, just not cautious.

Given the size and importance of the problem, creating this solution is not a matter of "if" but a matter of "when".

About The Author

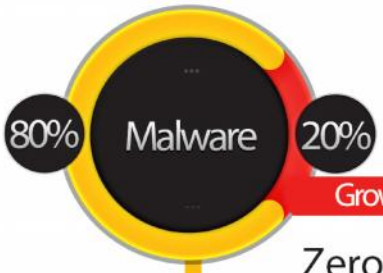
Chase Cunningham is the COO of CyberUnited, a leading security informatics company. Previously, he was the principle cyber threat analyst for the Neusentry Security Group at Neustar. He has 15 years in the security industry with all branches of the US Military, and spent 13 years as a Navy Chief Cryptologic Technician and cyber warfare operator supporting the US Navy Special Operations teams, as well as tactical Cryptologic Support teams from NSA. Chase holds numerous computer security certifications including Computer Information Warfare operator certifications, CHFI, Anti Terrorism Accreditation Board Cyber certifications and other industry specific security certs. He has specialized expertise in the areas of tactical cyber operations kinetic actions, intrusion detection, data mining, malware analysis, and red team operations.

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 ™

Twenty Critical CSIS Security Controls: Part Three

Malware Defenses and Application Security Controls

by Adam Montville, Security and Compliance Architect

Synopsis: *A former colleague used to carry on about how "the human" is really the new perimeter. In the case of CSIS Controls 5 and 6, that perspective rings very true. Humans relate to Control 6 in that the SDLC is, though aided by automation, largely a human-performed activity. Humans are the architects, designers, developers, and quality assurance folks. Humans run your source control management systems.*

In the first installment of this series we covered the “Inventory of Authorized and Unauthorized Devices” and the “Inventory of Authorized and Unauthorized Software.” In the second article we looked at two more Controls designed to offer guidance on managing secure hardware and software configurations on a variety of devices, as well as the implementation of continuous vulnerability assessments and remediation efforts.

It’s time to take a closer look at Controls 5 and 6 of the CSIS 20 Critical Security Controls which deal with malware defenses and application security, respectively (I consulted the PDF version, but the online versions are here and here).

Before getting started with the key take aways for Controls 5 and 6, I must reassert that each control we examine will include a set of requirements that you really should be taking directly to your security tool vendors. When you do, do not just take their word for it if they tell you they meet the 20 CSC requirements – make them really dig down and prove it to you. These controls are that important to your organization

Malware Defense Controls

In a Nutshell:

- Automation is Key: When it comes down to dealing with malware threats, automation is really the only way to go. The tools you use can be configured to automatically update signatures, learn from behavioral analysis, and work in tandem with other tools on the network. Of course, be sure that your antimalware systems are covered by your Configuration Assessment tools.

- Exercise Caution: Many recommendations made in this Control, could be cause for blowback in many organizations if implemented, such as blocking personal e-mail, instant messaging, and social networks in your environment. Realistically, most people are not so enthralled with their jobs that they don’t ever need some outlet during the workday to just break up the monotony. If you cut off the outside

world without a reasonable justification you will be considered nothing more than a prison guard. Nobody wants to be *that* guy.

- Begin with the Common Attack Vectors: It may be wise to begin by addressing the most common attack vectors, which are probably email and Internet traffic, then start looking at detachable media. Be very careful when it comes to blindly relying on configuration settings. Operating Systems like Windows are not as straightforward as they might appear. Make sure you have someone who really knows what they're doing here, or you may get yourself into trouble.

Areas for Improvement:

- Consider Different Perspectives: This is in direct relation to the second key take away above: Most Control Frameworks *only* consider the security perspective, and I believe security managers would benefit more from Frameworks if they approached issues more pragmatically. Most Frameworks are concerned with just one thing - security – and pay little to no attention to the real world issues security managers confront each day, such as the organization's business objectives. While a security-centric approach may be acceptable in specific environments like the government, finance, and energy verticals, it is not optimal in most others.

- Control Clean-up: Some of the requirements should be rewritten to make them clearer to the audience, and there are too many undefined and/or uncommon terms used which make the mandates difficult to understand. That should be an easy remedy.

- Add Some Specific Warnings: Many of the processes and tools mentioned or alluded to in this Control require specific expertise, and I would not rely on certifications alone when hiring for such positions. There are plenty of uncertified yet brilliant professionals available, but finding and vetting them can be laborious. If you don't feel comfortable doing the hiring yourself, there are some very qualified people out there who can help you.

For more details on this Control - including a numbered list containing each requirement, its description, and my notes pertaining to the requirements – refer to the full analysis here.

Application Security Controls

In a Nutshell:

- **Implement a Software Development Lifecycle (SDLC):** This might be better explained as a *Software Procurement Lifecycle*, because the Control addresses the operation of and the acquisition of application-level software.

- **Include Security Attributes in the SDLC:** Ensure that the SDLC is first of all performing the right activities, and secondly includes only qualified personnel. Doing static code analysis as part of the automated build/release process is good, but it's not a substitute for thorough manual code reviews by knowledgeable personnel.

- **QAs Should Examine for Common AppSec Bugs:** Qualified QA personnel should also be trained to attack application-level software and analyze SSL implementations, as well as having app-specific PKI deployment experience and input sanitization knowledge. QA personnel should be trained on the basics of security testing for applications, but there may be circumstances where a team of security assessors is needed to do the heavy lifting.

Areas for Improvement:

- **Split the Control:** There are two facets to this Control which would be better addressed separately. The first is the operational perspective as it applies to all application-level software, not merely software developed in-house. The second pertains to how you should develop in-house software. A good Software Procurement Lifecycle can be used for your in-house development, and a Software Development Lifecycle should be used to support that in-house development.

- **Define Terms.** Terms like "third-party-procured" - after reading through the control requirements a couple of, I still don't grasp what they mean by that and other loosely defined jargon.

- **Provide Examples for Standards:** CWE and CAPEC are referenced in the requirements as being beneficial for development and testing. The CWE use case is straightforward – we have a good taxonomy in the CWE dictionary at MITRE and more shops should use it. Using CAPEC to for test-tracking isn't so straightforward for most governed by this Control, so a simple an example would be useful. And if CAPEC is good for test-tracking, is there a tool that leverages it? Because development shops aren't likely to track things in raw XML.

For more details on this Control - including a numbered list containing each requirement, its description, and my notes pertaining to the requirements – refer to the full analysis here.

Conclusion

A former colleague used to carry on about how "the human" is really the new perimeter, and so forth. Well, in the case of Controls 5 and 6 that perspective rings very true. Remember, even though you've got your malware defenses automated and you have addressed common vectors, you shouldn't be "that security nut" who cuts off access to the rest of the world for your workforce - that's just counter-productive.

Humans relate to Control 6 in that the SDLC is, though helped by automation, largely a human-performed activity. Humans are the architects, designers, developers, and quality assurance folks. Humans run your source control management systems.

You will be interested in the forthcoming write-up on Control 9 (Security Skills Assessment and Appropriate Training to Fill Gaps) which will help ensure you're doing all you can to enable and empower your workforce to do the right thing.

About the Author: Adam Montville *is formerly a Security and Compliance Architect for* Tripwire Inc. *who ensured that technical architectures and solution capabilities solved real world security and compliance. Adam can be reached by email at* adam.w.montville@gmail.com *and on Twitter at @AdamMontville.*

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!

The Next Big Cyber-Crime Threat: Mobile

Cyber-attacks, insider threats, monetary fraud, and data breaches – affecting some of the world's leading organizations – make headlines every day. With attacks on enterprise networks becoming more sophisticated, organizations have stepped up perimeter security by investing in the latest firewall, data protection, and intrusion prevention technologies. As organizations improve defenses against direct networks attacks, hackers will move to the path of least resistance and look for new avenues to exploit.

The need to find new attack vectors initially led to a dramatic increase in targeted assaults on client-based applications, which use social engineering techniques against end users rather than looking for exposed servers at the perimeter. Hackers are now expanding their attacks even further to the edge by exploiting mobile applications to gain "backdoor" access to enterprise networks through BYOD. Security experts believe the next wave of enterprise hacking will be carried out via the mobile channel. In this context, it becomes essential to manage mobile application and device risks, and control their access to trusted networks. So what are the threats mobile / BYOD devices pose for organizations?

Understanding Mobile Threat Vectors

According to the ISACA® 2012 IT Risk / Reward Barometer, 72% of organizations in the U.S. are allowing (in one way or another) BYOD in the work environment. This new computing practice exposes businesses to unique risks that can threaten corporate security and reverse the productivity gains they were originally intended to deliver. Due to their portable nature and integration with public cloud applications, mobile / BYOD devices greatly increase the risk of data theft or leakage. In fact, a study by Decisive Analytics revealed that nearly half of the enterprises that allow BYOD to connect to their network have experienced a data breach.

Indeed, mobile / BYOD devices open up a whole new attack surface that hackers can use to target enterprise networks and the sensitive data they contain. Mobile devices can be exploited by attackers in several ways:

Malicious Attacks

Hackers use different techniques to launch malicious attacks against mobile / BYOD devices ranging from deployment of malicious software (viruses, worms, Trojan horses, and spyware) via a variety of infection methods (e.g., MMS, SMS, email, Bluetooth, Wi-Fi, user installation, self-installation, distribution via memory cards and USB), denial of services attacks (e.g., BlueSmacking, Bluejacking, SMS DoS, malformed OEBX message, malformed format strings, malformed SMS messages), to mobile messaging

attacks (e.g., SMS spoofing, SMS spamming, SMIShing, malicious contents messaging, SMS / MMS exploits).

Any of these can be used to carry out:

- Activity monitoring and data retrieval
- Unauthorized dialing, SMS, and payments
- Unauthorized network connectivity
- Data retrieval
- System modifications
- User interface impersonation with subsequent data exfiltration

All of these activities pose a real threat for any organization; especially if end users maintain their enterprise passwords on their mobile device.

Vulnerabilities

Vulnerabilities in the design or implementation of mobile operating systems and mobile applications exist that could expose a mobile / BYOD device's data to interception by hackers. With millions of mobile applications being promoted to end users, the risk of application vulnerabilities is exponentially high compared with other threat vectors. While the number of business application vendors is oversee-able, mobile application developers and sources are enormous and growing by the minute, prohibiting any type of trust or reputation assessment.

Vulnerabilities can lead to, but are not limited, to the following threats:

- Sensitive data leakage (inadvertent or deliberate)
- Unsafe sensitive data storage (e.g., banking and payment system PIN numbers, credit card numbers, or online service passwords)
- Unsafe data transmission (e.g., automatic connection to public Wi-Fi)
- Unauthorized permission requests

Questionable Privacy Practices

In addition to vulnerabilities, a large number of applications exhibit privacy practices that are concerning with respect to the manner in which they collect phone or location data as well as request data outside of the application sandbox. The fact that end user behavior is often based on the misconceptions that applications can't access their sensitive data or that they won't be hacked, only increases mobile risks. Finally, since very few mobile devices are protected by anti-virus software, Bluetooth and Wi-Fi are constantly being used, and sensitive information and files are stored in the mobile device memory, the job of protecting organizations against mobile security threats is

only getting harder. Given these challenges, what steps can be taken to maintain the productivity gains and cost-savings associated with BYOD, while proactively managing and mitigating security risks associated with this practice?

How to Manage and Mitigate Mobile Risks

The first and simplest practice is to implement an awareness program, educating mobile / BYOD end users about security threats and what actions to avoid. For instance, mobile devices contain lots of data but not all of it is sensitive. However, all an attacker needs is the right data to penetrate a secure network, such as email account credentials, user passwords, and corporate VPN login data. Furthermore, devices themselves can serve as a conduit directly into an enterprise network. For example, if a hacker infects a mobile device with malware, they could use the software to connect through the VPN to the internal network. Since many users connect their mobile devices via USB to their workstation, this could infect the network as well.

The second step is to establish rigorous policies around the usage of mobile devices – be they employer- or employee-owned. A good reference framework for this process are the "Guidelines for Managing the Security of Mobile Devices in the Enterprise", as propagated by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800-124 Revision 1. Establishing a mobile usage policy is the easy part. The hard part is gathering predictive risk information to determine, if, when, and how mobile devices should be able to connect to an organization's trusted network. In this context, many organizations rely on tools such as Mobile Device Management or Mobile Application Management.

While these tools offer rudimentary risk assessment and policy enforcement capabilities, they lack a comprehensive, real-time view of an enterprise's mobile and BYOD risk posture. Fortunately, new mobile trust services are emerging that can identify vulnerabilities at each layer of the mobile stack (infrastructure, hardware, operating system, and applications), correlate this data with existing threats, and score risks within the context of an organization's security ecosystem (e.g., use of security controls such as encryption, role-based access control, etc.). In turn, these risk scores can be used to determine whether or not to grant a device access to the network, and what, if any, limitations should be imposed. Once mobile access is granted, continuous monitoring can be used to maintain updated risk scores.

About the Author: Torsten George (tgeorge@agiliance.com) is Vice President Worldwide Marketing and Products at integrated risk management software vendor Agiliance. Learn more about him online at www.agiliance.com.

CYBER SECURITY SUMMIT 2013

SEPTEMBER 25

HILTON HOTEL

1335 AVENUE OF THE AMERICAS

NEW YORK CITY

Connecting C-Suite Executives with the Leading Cyber Solution Providers

FOR INFORMATION ON EXHIBITING OR ATTENDING VISIT:

WWW.CYBERSUMMITUSA.COM

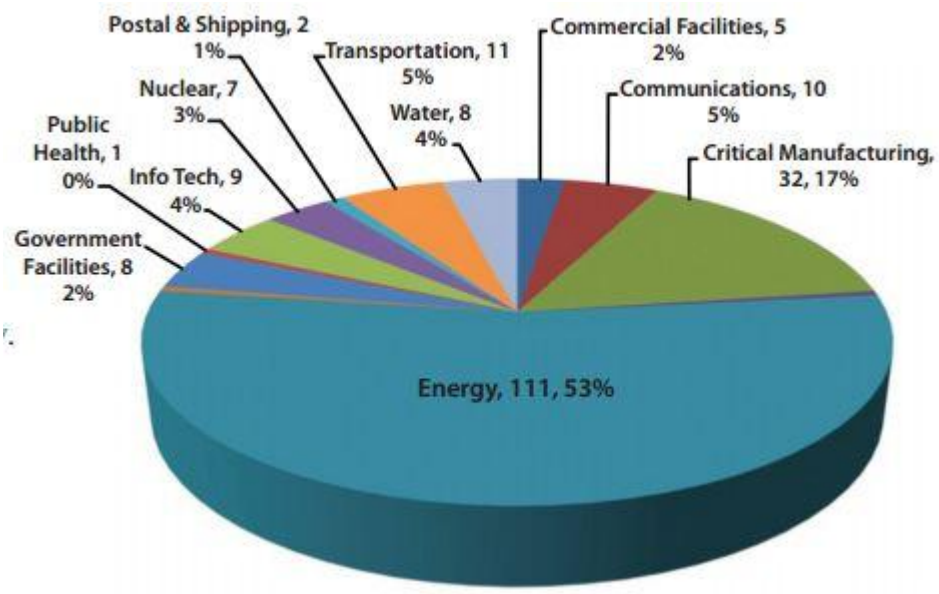
USE PROMO CODE CDM2013 FOR 50% OFF TICKET PRICES

ICS-CERT Reveals Energy Sector Brute Force Attack

The ICS-CERT issued a new Monitor report that revealed a surge of brute force attacks against control systems mainly belonging to the energy sector.

by Pierluigi Paganini, Editor-in-Chief

The ICS-CERT issued a new Monitor report that revealed an intensification for brute force attacks against control systems mainly belonging to the energy sector. The ICS-CERT received notification for more than 200 cyber attacks against critical infrastructure operators between October 2012 and May 2013.



Analyzing the sectors hit by the cyber attacks it is possible to note that 53% (111) of the offensives targeted control systems in Energy sector followed by Critical Manufacturing Industry at 17% (32).

Which kind of attacks hit the industries?

According the ICS-CERT the victims were targeted by mostly by watering hole attacks, SQL injection, and spear phishing.

ICS-CERT reported an increase of brute force attacks against a gas compressor station owner, the attack campaign fortunately didn't result in any actual breaches. The ICS-CERT issued an official alert on its secure portal about the attacks against the gas compressor plant providing also the 10 IP addresses being used in the offensives. The

attacks were concentrated against Gas compressor stations located in the Midwest and Plains region, they try to exploit weak or default passwords used to protect component of control systems exposed on the Internet, in the past numerous attacks of this type was notified to the ICS-CERT.

"On February 22, 2013, ICS-CERT received a report from a gas compressor station owner about an increase in brute force attempts to access their process control network. ICS-CERT posted an alert on the US-CERT secure portal (Control Systems Center), containing 10 IP addresses, to warn other critical infrastructure asset owners, especially in the natural gas industry, to watch for similar activity. That alert elicited additional reports from critical infrastructure owners who, using the indicators in the alert, had discovered similar brute force attempts to compromise their networks. Those new reports yielded 39 new IP addresses, which ICS-CERT included in an update to the original alert (also posted on the secure portal)," the *ICS-CERT states in its Monitor Report.*

Lila Kee, North American Energy Standards Board member highlighted the fact that ICS-CERT report is the demonstration of the concrete risk of cyber attacks against critical infrastructures and in particular against the energy sector. Kee confirmed the need to rapidly report that incidents and share data on attacks to prevent further damage.

"The report notes that the first half of 2013 yielded 200 brute-force cyber attacks, surpassing 2012's total of 198 attacks. Although attacks on major gas and electric systems are nothing new to those in the industry, these facts serve as evidence that low-level criminals, all the way up to state-sponsored groups, see the value in compromising our nation's critical infrastructure," Kee commented.

"Although the North American Energy Standards Board has done a fantastic job by drafting and recommending security standards, it is necessary that the critical infrastructure as a whole implement these standards to best apply preventative measures that prepare for the ever-increasing number and methods of targeted attacks," Kee added.

The majority of attacks according ICS-CERT occurs remotely, what is concerning in my opinion is that despite ICS-CERT analysts went on-site for five incidents in the first half of FY 2013 to investigate sophisticated incidents, in many cases their analysis was inconclusive because of limited or non-existent logging and forensics data from the ICS network

"While onsite, ICS-CERT analysts examined networks and artifacts to determine if ICS networks were also compromised. Unfortunately, in many cases that analysis was inconclusive because of limited or non-existent logging and forensics data from the ICS network," the report said.

The theme of cyber security for critical infrastructures is highly debated, cyber threats could hit foreign countries causing loss of human lives identically to a conventional attack, government are facing with a silently and unpredictable menace that could be conducted by state-sponsored hackers or cyber criminals with the different purposes, sabotage or cyber espionage.

Emergency Response Teams of every country are approaching the problem, they are working to complete a census of the structures examining their safety level, these groups of works are also working on awareness programs and information sharing, key activities to mitigate the risks.

Recently the U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT) has released a report that alerts on the increasing number of attacks against US critical infrastructure between 2009 to 2011, it is registered an impressive growth of the number of incidents, following its progression:

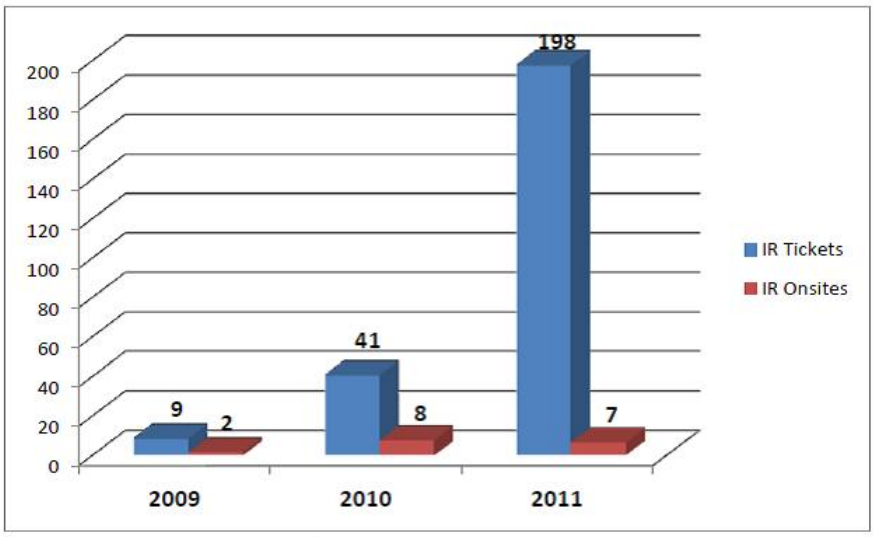


Figure 1. ICS-CERT incident response trends data.

The fact that the attempts were failed should not make us feel safe, the situation is critical and the level of alert must be high, cyber security of critical infrastructures is a must for any government like reinforced by this report.

"While none of the brute force attempts were successful, these incidents highlight the need for constant vigilance on the part of industry asset owners and operators. The ability to detect anomalous network activity and network intrusions early in an incident greatly increases the chance of a successful mitigation and resolution,"

The most common attack vector for network intrusion was spear-phishing, used for seven of the 17 incidents, critical is the risk assessment phase, according Lamar Bailey, director of security research and development at nCircle:

“We need a lot more collaboration between IT and security organizations to dramatically improve the accuracy of risk assessments.”

The guideline provided by the report are clear:

- Conduct detailed censuses of the structures and rated risk assessments to identify the main vulnerabilities and the cyber threats that could exploit them.
- Define, divulgate and adopt best practices to defend the critical infrastructures.
- To deal with spear-phishing firms must develop a security training program that will prepare the employees for the possible vector attacks and the main social engineering techniques.

In this scenario we will expect that the number of attacks will increase also in the next years, however the increased level of awareness and the high interest in the matter could avoid serious consequences.

(Sources: CDM, ICS-CERT, Cyber security)

A Quick Risk Analysis of B.Y.O.D.

Bring Your Own Device** Or **Breach Your Own Data?

Winn Schwartau, CEO, The Security Awareness Company

I am going to be blunt. The epidemic of B.Y.O.D. deployment is so fraught with obstacles that I believe a complete rethink of mobile consumerization in the enterprise is absolutely necessary.

My mobile security presentations often begin with a simple question:

> *"Do you want to be the first company to be sued for a Gazillion dollars because you chose to poorly implement and deploy your mobile workforce?"*

By the end of the decade, humans will share the planet with 20 billion intelligent IP endpoints. Phones, tablets, refrigerators, TVs, cars, Google glass and 'things' not yet invented will interconnect us personally with hundreds of global businesses to simplify and enhance our lives.

For now, though, let's only consider smart phones and tablets, to keep it a bit simpler.

As I have seen over thirty years in the security field, again we have chosen to deploy massive technological infrastructures – in this case mobile computing - without the forethought of embedded security.

Thus, we find ourselves in the position, once again, of figuring out how to add, bolt-on or duct-tape security features and functionality into a technology that enterprises have, somewhat reluctantly, adapted.

We did it for PCs and here we go again: listening to non-professional security vendors who sell anemic approaches that can only end in costly and embarrassing failure.

So, I am going to focus the very heart of the BYOD problem on risk. Are you, as the compliance/security officer, or as a Director, the CISO/CSO or risk management manager, willing to take the myriad risks associated with mobile? And put your name on it?

Keep in mind that mobile O/Ss are consumer devices. They are single user, non-multi-tasking and natively have about as much security as your TiVo. But it gets so much worse…

1. BYOD employs small, highly mobile devices. Studies show that 1 in 4 (25%) of your employees will lose their mobile device. That's more than 60 Million lost or stolen every year in the U.S. alone. Is that a risk you are willing to take? Would you accept it for your desktop computers?

2. MDM is not security. To be clear, MDM, in both iOS and Android, offers a compact set of tools for a fairly basic level of device management. However, despite the repeated erroneous claims to the contrary, MDM is a not a mobile security solution. If it were, your laptop security posture would be as follows:

    - Password length, complexity & duration controls.
    - Block adult materials.
    - Block browser and five Browser controls.
    - Erase laptop within 24 hrs. using native Active Sync.

That's it. That's all you get with MDM. MDM is explicitly removable by your users. It's part of the consumer design. MDM software can only be as secure as the underlying operating system. Is it worth the risk to pretend you have mobile security because a vendor sold you MDM? Would you allow this same approach to 'secure' your other devices that handle corporate data? Is it worth the risk? *Your* call.

3. MDM has been 'cracked' as evidenced by persistent cross-site scripting and cross-site request forgery vulnerabilities in two leading MDM solutions. Should you be using technology that can be bypassed or compromised as part of your security program? Is it worth the risk?

4. Containerization, aka sandboxing, is an attempt to allow both personal and company data on a consumer device. Do you allow co-mingled data on other business computers? Is it worth the risk… and is it worth the risk of lawsuits and compliance failures?

5. Container security such as Good Technology has already been broken. The jail breaking-rooting community will continue to find ways to crack this approach, as the underlying system is inherently not secure. MDM and Secure Containers both rely upon an assumed level of security and integrity in the device O/S. Given the vast number of unknowns, is using containers worth the risk?

6. Containers represent the antithesis of the reason companies are succumbing to the will of their new hires: “We want our Android…” (or iOS). Building a secure custom browser, email client and other containerized apps is not an easy build, and these give the user *anything but* the native device experience they so espouse. New apps present new risks; at least in my experience.

7. A containerized approach may offer some limited security for the corporate apps, but the user is then still left naked to interception and compromise. WiFi and carrier traffic are still in the clear. Bluetooth is open. Email credentials are broadcast. VoIP is not encrypted. Is the company guilty of providing a false sense of security to the user, who may not be savvy enough to know better?

8. An old (2009) Android ‘bug’ takes advantage of a so-called ‘Master Key’ allows malicious hackers to modify APK code without breaking the cryptographic seal. Thus legitimate apps can become infected and hostile apps can be signed with legitimate verification codes, potentially exposing all PII on a device, including corporate access rights.

(https://blog.cloudsecurityalliance.org/2013/04/25/how-secure-is-mobile-device-management-anyway/, http://techcrunch.com/2013/07/04/android-security-hole/, https://www.hackinparis.com/sites/hackinparis.com/files/MDM-HIP_2013.pdf)

Finally, let’s bring in the lawyers. You know and I know that with a set of newly defined risks, and so many big companies (read: deep pockets), lawsuits will raise the abysmally low bar of mobile security. How many? Oh, let us count the ways:

200 Chicago police officers have sued, claiming that the city owes them millions of dollars in overtime pay because they were required to answer work-related calls and emails during off hours.

If an employer expects employees to be connected and on-call 24/7, unless there is appropriate compensation, some subset of employees or their reps are going to sue.

As we moved from the two device Air Gap mindset into an attempted single device BYOD effort, has your organization considered the additional risks of litigation that is going to befall some number of companies in the near future?

- The company accidentally erases all of Granny’s LAST pictures from your phone. Who is liable and what is the risk?

- 25% of your employees are going to lose a mobile device this year. When a data breach occurs from loss or theft, is the company or the employee liable? Who carries the most risk?

- When a company's devices are subject to search and seizure in a legitimate law enforcement investigation, does the user have to hand it over just because some company resources sit on a personal device? Who is really taking the risk here?

- When a container is breached and very embarrassing personal data ends up with HR, who's going to sue whom? I can't even measure that risk!

- As a pure security professional, I am not a single device BYOD fan for so many technical reasons. The legal aspects are the justice system's way of monetizing poor security design and practice.

	BYOD	Air Gap
Personal/Business data completely isolated?	Yes	No
Personal Prvacy in jeopardy?	Yes	No
Employee risk of losing company data?		
Compliance Risk?	Yes	No
Company potentially liable for personal data loss?	Yes	No
Who is liable for breached company data?	Unknown	The Company
Who is liable for compromised personal data?	Unknown	Not Applicable

Does decent mobile security exist?

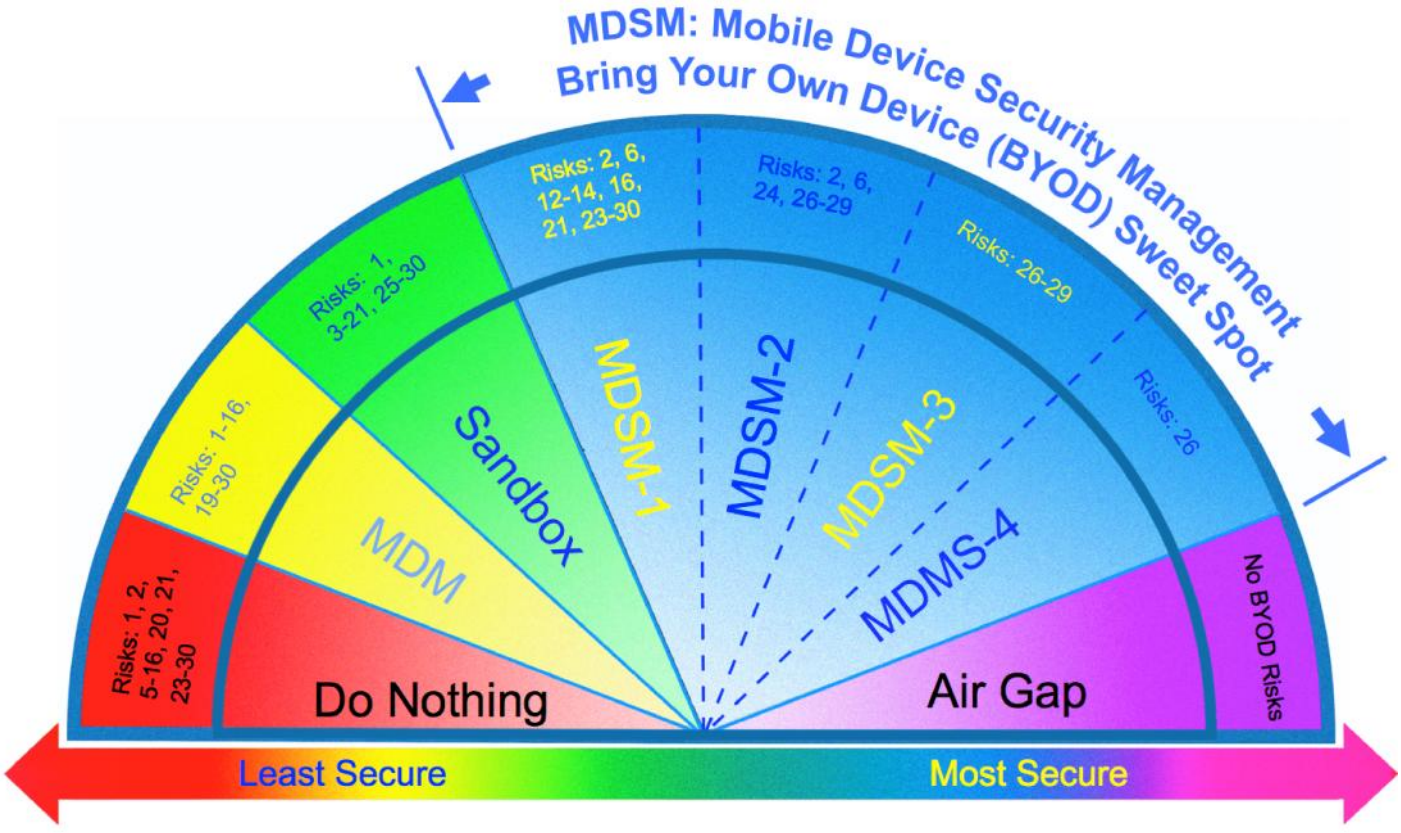
Yes, but you're going to have to either build it yourself, or find the one or two vendors who have actually done it.

I see no reason mobile security should be any less stringent (it should be more, actually) than organizations enforce in their fixed enterprises. I would like to hear from people who think that a secure mobile enterprise should *not* include: Always-on IPSec VPN for WiFi and Carrier, VPN Concentrator- with strong firewall controls, content filtering, SIEM, DLP, IPS, jailbreak detection, strong remediation and an extensible policy.

Please tell me why I, or any company, would not want these security features in a hostile mobile environment.

The following charts show the complete BYOD Security Spectrum, analyzed from a risk perspective, which you may find useful in truly categorizing and weighing your current and/or future mobile security efforts.

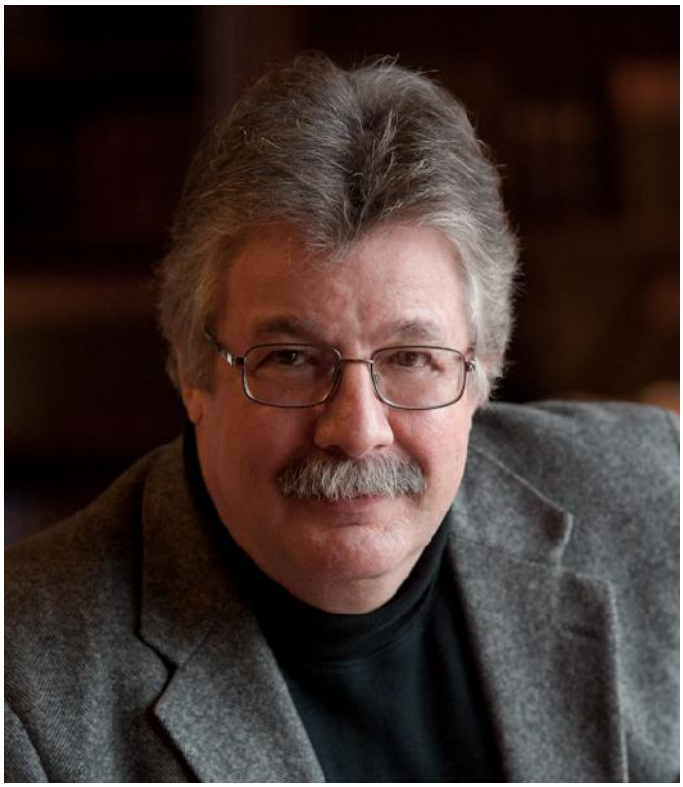
Finally, and to the point of near absurdum, studies have shown that single device BYOD programs using MDM and containers costs the company between 1.7 – 4 X the historical costs of using two devices: One for work and then whatever the employee wants for his personal use.



You might think me harsh in my comments. But think about the mistakes we made on PC and internet security over the last three decades. Were they, in hindsight, worth the risk and the costs?

If you choose to ignore history and repeat the same mistakes again, please raise your hand.

Risk ID #	Mobile BYOD Risk Description	Do Nothing	MDM	Sandbox	MDMS-1	MDSM-2	MDSM-3	MDSM-4	Air Gap
1	Risk of Password & Credentials Interception	x	x	x					
2	Risk of Comingling Personal & Company Data	x	x		x	x			
3	Risk of User Bypassing/Diabling Security Controls		x	x					
4	Risk of ID Spoofing (Unknown Devices) and Audit Control (no-CA)		x	x					
5	Risk from No Trust Model	x	x	x					
6	Risk of Company Data Breach	x	x	x	x	x			
7	Risks of WiFi Data Eavesdropping	x	x	x					
9	Risk of Carrier (3G/4G) Data Interception	x	x	x					
8	Risk of VoIP Interception	x	x	x					
10	Risk of Application Data Eavedropping	x	x	x					
11	Risk from Lack of IDS/IPS & Remediation	x	x	x					
12	Risk from Phishing	x	x	x	x				
13	Risk of Malware Breaches	x	x	x	x				
14	Risk of Malware Download	x	x	x	x				
15	Risk of No Device Lock Down or Mobile Firewall	x	x	x					
16	Risk of Becoming Part of Mobile Botnet	x	x	x	x				
17	Risk of User Misusing Non-Native Apps			x					
18	Risk of User Error in App Configuration			x					
19	Risk of Man in the Middle Attack (for SSL VPNs)		x	x					
20	Risk of Mobile IP Address Scraping (NAT)	x	x	x					
21	Risk of Falling out of Regulatory Compliance	x	x	x	x				
22	Risk of Delayed Active Sync Response		x						
23	Risk of 3rd Party Data Exposure from Lost Device (FDE)	x	x		x	x			
24	Risk of Company Liability for Loss/Disclosure of User Data	x	x		x				
25	Risk of BYOD Breaches	x	x	x	x	x	x	x	
26	Risk From Device Policy Not Changing With Device Location	x	x	x	x	x	x		
27	Risk of Violating Policy When Travelling to Restricted Locations	x	x	x	x	x	x		
28	Risk of Exposing PII When Not on Premises (Fin., Med, Gov, etc.)	x	x	x	x	x	x		
29	Risk of Not Using DLP	x	x	x	x				
30	Risk of Inadequate audit and forensivs records (SIEM)	x	x	x	x				



BIOGRAPHY: WINN SCHWARTAU

Winn Schwartau thinks asymmetrically and has been "Security" for almost 30 years. As he puts it, "I've been in security for about 30 years and I think, maybe, I'm just starting to understand it."

If you want originality in thought, writing, presentations or any aspect of Security, call Winn. In addition to being called, *"The Civilian Architect of Information Warfare,"* he is one of the country's most sought after experts on information security, infrastructure protection and electronic privacy. http://en.wikipedia.org/wiki/Winn_Schwartau and www.WinnSchwartau.Com

Career Overview

Experience, Affiliations and Notable Accomplishments

- Founder, **www.SecurityExperts.Com** (Opening 4Q 2012) A "Spare Time" pet project.
- Chairman, **Mobile Application Development Partners, LLC,**
- **Distinguished Fellow: Ponemon Institute**
- In November 2009, was named one of the **Top-20 security industry pioneers by SC Magazine.**
- Named one of the **Top 25 Most Influential People** for 2008 by **Security Magazine**
- Voted one of the **Top 5 Security Thinkers for 2007** by **SC Magazine.**
- In 2002, honored as a **"Power Thinker"** and one of the **50 most powerful people** by **Network World.**
- Named a **Ponemon Institute Fellow**, 2012.

Full Bio available at: (http://www.winnschwartau.com/about.html)

Inside-Out Attacks: How Malicious Hardware can Siphon Your Data

Cyber attackers are technically sophisticated, well financed and have significant resources at their disposal according to the Mandiant 2013 Threat Report. While recent Internet attacks against financial institutions that knocked their websites offline garnered headlines, there is growing concern in the security community regarding threats that can be perpetrated on physical hardware. Two specific techniques can be used in these type of attacks. One involves malicious hardware and the second requires pre-installing malware on the target system.

What can a malicious hardware device do? These can be engineered to extract or modify the contents of main memory in a computer, which typically contains sensitive data as well as system information. For example, by taking a snapshot of a server's memory and parsing its contents, an attacker can extract digital (SSL) certificates, or encryption keys to unlock data-at-rest.

Hardware devices that can extract data are not difficult to engineer. A simple internet search on "malicious hardware" yields a wealth of research and information on the topic. Malicious hardware devices can take advantage of most computer interfaces including USB and Firewire ports on a PC and PCIe slots on a server. Bad actors can design hardware for these interfaces to extract data from a computer. These devices can be installed by rogue insiders or even inadvertently since very few organizations have the resources to test and validate hardware purchased from vendors.

Vulnerabilities can also exist in hardware being installed in IT infrastructures. This became apparent last year with news reports about new laptops being shipped from manufacturers' factories pre-installed with malware. Meanwhile, a January 2013 Department of Defense Science Board task force report warned that "U.S. networks are built on inherently insecure architectures with increasing use of foreign-built components".

We recently performed vulnerability research on the Linux kernel and found that within a sample of Linux network drivers, 50 percent were vulnerable to code injection attacks. Since there are eight million lines of device driver code in the Linux kernel, this represents a very large attack surface. If bad actors can modify device drivers, they can just easily create bootkits that can compromise server information without detection.

Accessing a PC or a laptop is relatively straightforward, but most sensitive data resides on servers located in enterprise datacenters, at hosting/co-location facilities or in cloud service provider environments. Nevertheless, anyone with physical access to a server can install malicious hardware on the system to extract information. So while background checks can help minimize the risk of rogue employees stealing confidential information, one hundred percent reliability is impossible as recently illustrated by Edward Snowden.

So, what can be done to reduce the threat of malicious hardware being used to siphon confidential data? Here are three measures to consider:

Audit the IT supply chain including firmware: Audit the firmware of your servers and interface cards before installing them. Some organizations such as government and financial institutions already have such supply chain risk management processes in place.

Start using server attestation technologies such as Intel Trusted Execution Technologies (TXT) to validate software and firmware, and to detect the presence of bootkits or rootkits. TXT is capable of conducting static and dynamic root of trust measurements, which will reveal malicious changes to software or firmware. Utilize technologies that can identify registry software and driver changes that might indicate the system has been compromised by a rootkit.

Secure Data In Use: Evaluate technologies that encrypt server memory and data-in-use. Since data in memory is "in the clear" it can be can stolen by malicious hardware devices, even if data at rest encryption is in place. Attempts to use direct memory access (DMA) and memory extraction techniques against physical systems that use full memory encryption would be ineffective.

Contrary to popular belief, encrypted data, whether in the cloud, a hosted environment or an enterprise datacenter can still be accessed, stolen, and copied. One of the primary vectors for undermining data at rest and SSL encryption, as well as other data protection mechanisms, is through the use of malicious hardware to compromise data in-memory. Fortunately, advances in microprocessor and virtualization technologies are spawning solutions that can provide this missing layer of protection.

Todd Thiemann is vice president for marketing at data encryption provider PrivateCore where he is responsible for all marketing activities.

He has over 20 years of experience in data protection, data center security, enterprise system market segments. Todd is also co-chair of the Cloud Security Alliance Solution Provider Advisory Council.

Top Seven Things You Should Be Thinking About The NSA Spying On You

by Gary S. Miliefsky, CISSP®

I remember sitting on the airplane next to Dan Brown's professor who told me the story of what inspired Dan to write Angels & Demons and then The Davinci Code. Dan had a few students show up late to class and the story goes that they sent an email jokingly that included a potential threat to the President's life at that time and the Secret Service 'magically' showed up and interview them for a while, delaying their attendance in class. Dan heard it all 'the dog ate my homework', 'it went into the washing machine', etc. but he never heard 'sorry prof. we're all late for class because an email sparked a visit by the US Secret Service'. So he dug into it and found out a) they were NOT lying and b) it was happening back then - all of our emails being devoured by 'carnivore' - the codename for the first NSA system that would dig into all emails looking for keywords.

Having helped out in the development of the Whitehouse Plan to Secure Cyberspace, many years ago, I can tell you that our government has known it has many weaknesses - including the Office of Management and Budget (OMB) giving out Cyber Security grades - remember when the US Department of Education received an "F" - that's a failing grade at securing their networks against attack? So our government continues to take proactive steps to harden the myriad of networks it uses each day to get business done, defend our nation and provide services to our citizens. In addition this sparked the fuel for initiatives like Total Information Awareness (TIA) to dig more deeply into the Internet, in real time.

The NSA has been spying on all of us for a long time. Allegedly it's their job – we'll not to spy on you or me, just those bad guys out there and not knowing who they are, why look for a needle in a haystack when you can just takeover the entire haystack, right? Now, suddenly its front page news. Here's an example, without needing a warrant - if a person in the USA calls a person in another country - say Saudi Arabia, and they talk about attacking America, the 'other side' of the call can be tapped without a warrant and eavesdropped as the other party is not in America and most likely not an American citizen. So that's where it starts to get fuzzy.

Then, as our government continues to expand, folks believe they need to create more programs, deliver more tools - to automate, to store data for forensic purposes and the list goes on. So we go from a tiny spigot of spying into a flood of eavesdropping on everything - all phone calls, all emails, soon all internet searches, all facebook messages, all tweets, all linkedin notes and the list goes on. Will this stop a terrorist attack? No. It's like my friends in the police departments tell me - 'they call us knowing it could take up to 12 minutes to arrive - we usually show up to clean up the mess' - of course that's why even Joe Biden wants you to at least have a shotgun - it's an instant equalizer while you wait 3-12 minutes for help.

So the NSA decided to not wait around for someone to test the true Constitutionality of their efforts - they felt it was in the best interests of the citizens if they could spy on all of us, hoping to find that one needle in a haystack...correction, allegedly 50 terrorist needles in a haystack of 330,000,000 Americans in a world of 6,500,000,000 people. I can't tell you if the stories are real because it's hard for an agency that has highly classified information to share anything with us that's true. Lots of reasons why - don't tip the enemy, etc.

Where does that leave us? Not feeling so good about being spied upon. The real reason is that when organizations grow to the size of the NSA, there's more than just Whistleblower risk - there's bad apples in the bunch. We've had Chinese government spies working at Los Alamos for heaven's sake! Imagine you have that kind of power - to tap into a data source for everything on everyone...what's out there but a secret tribunal to protect us? Is that good enough? Many Americans are beginning to question this and size it up against the 1st, 2nd, 4th and 5th amendments saying that their rights are being trampled in the name of security. Remember, as one of our Founding Fathers' said "A society that's willing to give up Liberty for Security shall have Neither." This is the warning cry.

So with that all said, what are the Top Seven Things you should be thinking about The NSA Spying on You:

1) Do you believe it's important to give up Liberty for Security?
2) Do you believe there's enough oversight into these programs?
3) Did you know it's been going on for a very long time?
4) Do you think your Congressperson cares enough to defend your Liberty?
5) Do you think trying to 'go off the grid' will really work for you?
6) Will an Aluminum hat and a CB radio or HAM radio be the right answer?
7) Did you Know That Cyber Criminals and Other Nations are Spying on you as well through your laptops, tablets and smartphones?

It seems to me that you have to call and write your Congress folk to tell them you either support the NSA's ever expanding web of real-time eavesdropping on everything they can about you - where you work, what you say and do, where you shop, what you buy, what you say online, who you say it to, etc. or that you don't support it. Maybe the big question will lead to better oversight and declassification of some aspects of these programs? Maybe with trillions in debt, some of the costs of these programs should be looked at more carefully?

As to getting off the grid - it's really too late. The fact that you do it is information in itself and may put you on a list to be scrutinized even more closely...hence the newly purchased drones flying around US airspace? I'm sure you are not a terrorist and have nothing to hide but that doesn't mean someone in the government doesn't flip the bit from zero to one and you get the quiet black helicopters and whizzing drone flybys on a more regular basis.

What's even more disconcerting is the fact that we all download apps on our mobile devices and click 'trust' without ever verifying their trustworthiness. Does Facebook app on Android, for example, really need access to your Microphone, Webcam, GPS, Contact List, Constantly Polling over the Internet (for what reasons?) and that's from an apparantly good company. How about installing antivirus from NQ Mobile thinking they are going to clean your device when they have a very shady past, being founded in China and kicking off sales by fixing malware that only they could discover (later admitting that they hired the malware writer as a consultant for allegedly other purposes....hmmm...).

How about the recent version of Angry Birds that was infected and spamming through your Contacts list and SMS paging? What if one of these thousands of apps on the Microsoft, Google or Apple marketplaces are spying on you right now? How would you know? What if an online predator is watching your children through their tablet's webcam, listening in on the microphone and geo-locating them while they are home alone with a 16 year old babysitter? This does happen and the eavesdropping software to do it is freely available on the internet. You did click trust on that funny named applet you wanted the kids to play with, didn't you? What about your bank account information on your Smartphone being stolen over bluetooth by a nearby hacker or someone who bumps into you on the train gets it from your Near Field Communications (NFC) protocol that's always running on your device but you didn't even know, did you?

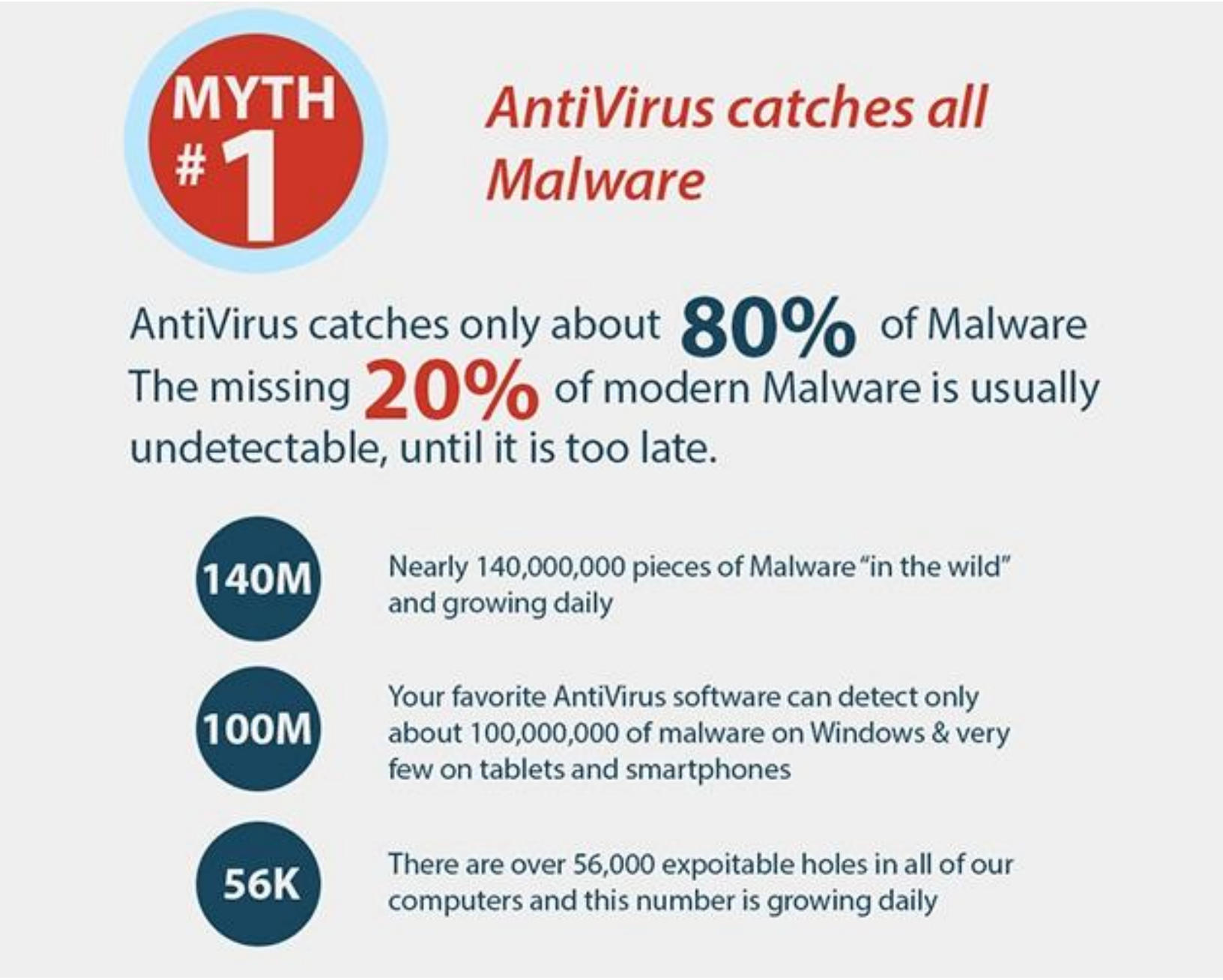
It's time to take control of our laptops, tablets and smartphones. It's time to begin to reclaim our privacy. There hasn't been a way to do it yet. There may be soon, as I'm actually working on it through my new project at www.snoopwall.com. Until then, maybe the experts are right - put tape over the webcam and microphone and please, do remove the batteries when not making a phone call. Also, tell the kids to play Scrabble...it's much safer, for now.

About the Author

Gary is the President & Founder of SnoopWall and the sole inventor of the company's new technology. He has been active in the INFOSEC arena, most recently as the Executive Producer of Cyber Defense Magazine and prior cover story author and prior contributor to Hakin9 Magazine. He founded NetClarity, Inc., an internal intrusion defense company, based on a patented technology he invented. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. He advised the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http://www.NAISG.org). Email him at: garym@snoopwall.com

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)

Cyber Intelligence Europe, Brussels, Belgium, 17th – 19th September

Cyber Security is an ever growing topic that many European Government Departments are taking seriously, by investing heavily in securing their critical infrastructure and sensitive information. There is now a greater need for European Governments to take cyber security more seriously and to have the correct security/intelligence in place before they are attacked.

Many Governments are looking to co-operate with the private sector to help them secure their infrastructure and cyberspace as many government/military computer systems are becoming integrated and layered making it significantly harder to secure from a cyber-attack. This event will provide you with an overview of Government cyber security strategies and challenges, providing a great opportunity to develop and learn more about how the public sector maintain and manage their ever growing computer systems. Join us at our inaugural Cyber Intelligence Europe event to hear in-depth and knowledgeable presentations from the public and private sector on cyber security issues and trends from their perspective countries.

Speakers include:

- **Major General Roar Sundseth,** Chief Information Officer and Commanding General of Cyber Defence, **Norwegian Armed Forces**
- **Suleyman Anil,** Head of Cyber Defence, **NATO ***
- **Troels Oerting,** Head of European Cybercrime Centre (EC3), **EUROPOL**
- **Guiseppe Abbamonte,** Head of Unit, Trust and Security, DG-CONNECT, **European Commission**
- **Dr. Udo Helmbrucht,** Executive Director, **European Network and Information Security Agency (ENISA) ***
- **Omar Sherin,** Director, Critical Infrastructure, **Qatar Computer Emergency Response Team (Q-CERT)**
- **Senior Inspector Ljuban Petrovic,** Cyber Crime Investigator, Service for Combating Organized Crime, Cyber Crime Department, **Ministry of Interior, Serbia**
- **Samir Mukhtarzadeh,** Senior Detective Officer, Cybercrime Unit, **Ministry of National Security, Republic of Azerbaijan**
- **Francesca Bosco,** Project Officer, **United Nations Interregional Crime and Justice Research Institute (UNICRI)**

Don't miss out on the chance to hear from a wide international perspective on topical sessions on European Cyber Security Strategies & Policies, Cyber Law, Emerging Cyber Threats, Combating Cybercrime and International cooperation and collaboration.

If you are interested in participating at please contact events@intelligence-sec.com

- Listen to the key European players in the cyber security industry
- Opportunity to network with 150+ delegates from across the globe
- Discuss the latest cyber security challenges and emerging threats
- Analyse the latest solutions to stop cyber terrorism with esteemed government personnel
- Take the time to visit the vibrant exhibition to learn the industry solutions to cyber security
- Don't miss the chance to be networking with senior cyber experts for a full 3 day event

NSA Spying Concerns? Learn Counterveillance

Free Online Course on August 12, 2013 at www.concise-courses.com

"NSA Spying Concerns? Learn Counterveillance" is a 10-minute live 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.

Stay tuned for the direct URL to this upcoming event and bookmark http://www.concise-courses.com

Cyber Warnings Newsflash for July 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…

6,300 USC students warned about data breach

06/28/2013 11:29 (TheState.com)

...that time period was on the laptop. The password-protected **computer** included names and Social **Security** numbers of students who took the classes,

Cyber security in the classroom

06/28/2013 10:18 (KSDK)

Cyber security in the classroom By Sharon Stevens, Education Reporter CLAYTON, Mo. (KSDK) - The threat of cyber attacks is a sign of the time...

Opera developers explain why malicious update wasn't detected

06/28/2013 10:09 (Help Net Security)

the theft of an expired code signing certificate, and the delivery of **malware** signed with it through the auto-update mechanism to Opera users.

Most Internet users have fallen victim to malware

06/28/2013 09:11 (Help Net Security)

Most Internet users have fallen victim to **malware** The current state of **cyber**-**security** has left US Internet users anxious about hacks and password...

Retired General under investigation for leaking 'Stuxnet' cyber attack details

06/28/2013 07:54 (New York Post)

Retired General under investigation for leaking '**Stuxnet**' **cyber attack** details WASHINGTON A former vice chairman of the Joint Chiefs of Staff...

Abuse of mobile app permissions

06/28/2013 07:21 (Help Net Security)

...get consumers to agree to invasive permissions that allow scammers to deploy **malware**. The permissions in free apps, funded by adware, leak personal...

3 reasons why America's security model is broken

06/28/2013 05:52 (Computerworld)

...secure. Just look at the headlines, whether it is Anonymous latest **attack**, state sponsored **Cyber** espionage or warfare, criminal activity or just someone...

US military to review cyber crime dealing rules in face of increased threat

06/28/2013 04:03 (Albuquerque Express)

US military to review **cyber crime** dealing rules in face of increased threat The US military has decided to review its rules of dealing with cyber...

Pentagon investing in cyber to stop growing attacks

06/28/2013 02:52 (Daily Record (AP))

Pentagon investing in **cyber** to stop growing attacks WASHINGTON - The nation's top military leader said the number of **cyber** intrusions probing...

Stop hijackers of your domain

06/28/2013 01:17 (Northern Colorado Bussiness Report)

are both time-consuming and costly. According to the National **Cyber Security** Alliance s 2012 National Small Business Study, 66 percent of businesses...

State computers compromised, not enough staff to fix it

06/28/2013 00:40 (Yahoo! News Canada)

The next frontier of application context-awareness: mood

06/27/2013 22:59 (Computer World Australia)

...'HP is here to stay,' CEO Whitman tells ... Google adds **malware**, **phishing** numbers to its transparency ... ING Direct unveils new mobile banking...

Governments should focus on cyber security for critical infrastructure

06/27/2013 22:42 (Computerworld Malaysia)

Governments should focus on **cyber security** for **critical infrastructure** Robust **security** strategies include policies, education, training, and...

UK users hit with 3,000 phishing attacks per day, says Kaspersky Lab

06/27/2013 22:17 (Computer World Singapore)

UK users hit with 3,000 **phishing** attacks per day, says Kaspersky Lab UK Internet users were subjected to 3,000 **phishing** attacks per day in the...

Cyber attacks threat to national security and business

06/27/2013 22:16 (Computerworld Malaysia)

Cyber attacks threat to national **security** and business More than half of all businesses believe **hackers** are already inside their networks, as...

Splunk moves on Hadoop analytics

06/27/2013 21:32 (Computer World Australia)

...'HP is here to stay,' CEO Whitman tells ... Google adds **malware**, **phishing** numbers to its transparency ... ING Direct unveils new mobile banking...

Android malware devlopment now mimics commercial software, claims Juniper

06/27/2013 21:26 (Computerworld Malaysia)

Android **malware** devlopment now mimics commercial software, claims Juniper Discovers **malware** peak around Christmas. The creation of Android **malware**...

Cybercrime fueled by mature digital underground

06/27/2013 20:47 (Computerworld Malaysia)

...disclosure that more than 50 million records compromised in April 2013. **Malware**. Fraud apps are typically used to impersonate a victim or gain...

U.S. to press China on cyber theft: Lew

07/01/2013 05:27 (Yahoo! News Canada)

Firewalls in firing line as US military plans data-centric network

06/30/2013 23:26 (Computer World Singapore)

Firewalls in firing line as US military plans data-centric **network** The US **Defense** Information Systems Agency (DISA) is planning a complete overhaul...

More than 50 percent of consumers say they've been victimized by bad apps

06/30/2013 22:58 (Computer World Singapore)

...victimized by bad apps More than half of consumers have been victimized by **malware** or a **computer virus** and more than a third have been targeted by...

New disk wiper malware linked to attacks in South Korea, researchers say

06/30/2013 22:07 (Computerworld Malaysia)

New disk wiper **malware** linked to attacks in South Korea, researchers say The **malware** is similar to the one used against South Korean banks and...

Google's Transparency Report boosted by malware and phishing numbers

06/30/2013 21:34 (Computerworld Malaysia)

Google's Transparency Report boosted by **malware** and **phishing** numbers Firm admits it still underestimates the problem. Google has bolstered its...

Two malware programs help each other stay on computers

06/30/2013 21:20 (Computerworld)

Two **malware** programs help each other stay on computers Microsoft says the Vobfus and Beebone malicious software programs are proving to be a...

Snowden's Leaks Cloud U.S. Plan to Curb Chinese Hacking

06/30/2013 20:47 (Bloomberg)

...he believed that such a step now -- amid the furor over the National **Security** Agency s **cyber**-espionage -- would lose much of its punch. The same...

"Old" Malware Attacks Rising Significantly

06/30/2013 16:55 (Examiner.com - Massachusetts)

Old **Malware** Attacks Rising Significantly Earlier this week McAfee Labs released the McAfee Threats Report: First Quarter 2013, which reported...

Cyberattackers are flying under radar

06/30/2013 00:36 (The Free Lance-Star)

...stores and even the city of Sacramento, Calif., have had their **computer** systems hacked or **compromised**. It s part of a shift from mass attacks...

Cyber Report: Attackers on Network

06/29/2013 10:48 (Isssource.com)

...physical attacks. 61 percent of respondents believe that **government** and legislative action can help protect critical infrastructure against advanced...

Stuxnet inquiry targets general

06/28/2013 18:48 (Tribune-Review (AP))

Stuxnet inquiry targets general Updated 15 minutes ago A retired four-star Marine Corps general who served as the nation's second-ranking military...

Trojan Speaks Local Languages

06/28/2013 18:06 (Isssource.com)

Trojan Speaks Local Languages A Citadel **malware** variant is capable of delivering fraudulent web pages automatically customized to the language...

'DarkSeoul' Behind S. Korea Attacks

06/28/2013 17:52 (Isssource.com)

...Korea have always been multi-staged. In addition, the destructive **malware** payloads such as the distributed denial of services (DDoS) attacks and...

Mobile Malware Threats Up 614%

06/28/2013 17:37 (Isssource.com)

Mobile **Malware** Threats Up 614% The number of mobile **malware** threats increased by 614 percent from March 2012 to March 2013, a new report said.

Despite security fears, most Americans don't use two-factor authentication

06/28/2013 14:46 (Infosecurity)

...little more than half (56%) of consumers have been a victim of a **virus** or **malware** infection on a **computer**; 37% have been a victim of a **phishing**...

MI5 and GCHQ: Britain facing 70 advanced cyber attacks per month

07/02/2013 04:24 (Infosecurity)

...advanced cyber attacks per month The UK s MI5 and the **Government** Communications Headquarters (GCHQ) have revealed that according to their information-gathering...

Guest View: Matching protection criteria to the next wave of threats

07/02/2013 04:00 (Computer World Singapore)

...rootkits. Today we find ourselves combatting the latest wave - advanced **malware**, targeted attacks and advanced persistent threats (APTs). While...

The biggest security snafus of 2013 (so far)

07/01/2013 23:55 (Computerworld Malaysia)

...the data. - Restaurant chain Zaxby's Franchising said it found **malware** on the systems of many of its restaurants after it was notified of potential...

Sourcefire upgrades security platform

07/01/2013 23:55 (Computerworld Malaysia)

...planning. Sourcefire recently announced that it has upgraded its **cyber security** platform to include features that will give organisations the...

Passwords aren't dying any time soon. Here's how to manage them effectively.

07/01/2013 22:27 (Computer World Singapore)

...value of two-factor authentication, passwords remain the primary means of **digital security**. They're also one of the weakest links in the security...

Critical infrastructure protection: Are we prepared for a massive cyberattack on U.S. systems?

07/01/2013 21:57 (Computer World Singapore)

Critical infrastructure protection: Are we prepared for a massive cyberattack on U.S. systems? There is no debate in the security community that...

South Korea hit by disk wiping attack blamed on 'DarkSeoul' gang

07/01/2013 21:37 (Computerworld Malaysia)

...same success, probably because it is a fairly crude piece of **malware** with low distribution. Defences have also been tightened up since the earlier...

SBA relying on shared services to improve cyber posture

07/01/2013 20:53 (FederalNewsRadio.com)

...over the last year the 802.1x standard to improve its **network defense**. The standard secures an organizations network ports by applying access...

Energy Industry Top Attack Choice

07/01/2013 19:09 (Isssource.com)

...ended up hit mostly by watering hole attacks, SQL injection, and **spear phishing**. In fiscal 2012 alone, 198 cyber incidents ended up reported...

Bulgarian Faces Hacking Charges in NJ

07/01/2013 17:51 (Isssource.com)

Symbiotic malware work together to avoid anti-virus detection

07/01/2013 15:48 (Infosecurity)

Symbiotic **malware** work together to avoid anti-virus detection **Malware** known as Win32/Vobfus works in a symbiotic relationship with other **malware**,

Phishing surge shows human element weakest link in cyber-defense

07/01/2013 15:48 (Infosecurity)

Phishing surge shows human element weakest link in **cyber**-**defense** Although the key part of the term **cyber**-**security** is certainly the **cyber** portion,

Android hack tool harvests info from PCs

07/01/2013 15:13 (Help Net Security)

...from PCs Stealing information is a piece of cake if you can manage to get **malware** on the target's Windows computer, but did you know that it can...

Combating attacks with collaborative threat intelligence

07/01/2013 13:32 (Help Net Security)

...Advanced Persistent Attacks (APTs) get most of the attention from the **cyber security** community because, as defenders, we want to be vigilant against...

Malaysian editions of corporate websites affected by 'DNS poisoning'

07/01/2013 10:45 (Computer World Singapore)

...- in this case to a defacement site. This incident is not related to **malware** infection but is an issue related to a DNS [domain name system,]

Beware of "Social Security" Facebook phishing scams

07/01/2013 10:25 (Help Net Security)

Beware of Social Security Facebook **phishing** scams Hijacked Facebook Fan Pages are a great asset to online spammers and scammers, so it's no wonder...

Google to release data on malware

07/01/2013 10:08 (The Journal Gazette)

Google to release data on **malware** Google said it will begin to regularly publish Internet security data on **malware** and **phishing** scams that infect...

Alert: Malaysian websites including Microsoft's hacked

07/01/2013 08:47 (Computer World Singapore)

...- in this case to a defacement site. This incident is not related to **malware** infection but is an issue related to a DNS [domain name system,]

33% of CEOs vulnerable to spear-phishing attacks

07/01/2013 07:28 (Infosecurity)

33% of CEOs vulnerable to spear-**phishing** attacks Getting senior management on board is essential for an effective security policy; but new figures...

Teaching a computer to play Memory advances security

07/01/2013 00:08 (Help Net Security)

Teaching a **computer** to play Memory advances **security Computer** science researchers have programmed a computer to play the game Concentration (also...

Nature, profile of cyber attackers known through digital forensics: report

07/03/2013 02:46 (Computerworld Malaysia)

Nature, profile of **cyber** attackers known through **digital forensics**: report **Cyber** attackers leave **digital** bread crumbs that can be traced. A new...

State AGs say Google profits from harmful YouTube videos

07/03/2013 02:28 (Computerworld Malaysia)

...sexual abuse imagery, and certain links to copyrighted material, spam or **malware**, as it is for courts and lawmakers and not Google to determine...

Windows 8.1 'smart search' will show you Bing ads

07/03/2013 00:52 (Computer World Singapore)

...that appear outside of the context of the browser are a good sign that **malware** is present. But these will appear within the context of an app,

With a simulated attack, Wall Street gears up to combat virtual threats

07/03/2013 00:00 (TheDay.com (AP))

a major financial industry group, will coordinate a July 18 simulated **cyber attack** with about 50 firms in an exercise called Quantum Dawn 2.

CTO signs pact for cybersecurity with global security alliance

07/02/2013 22:04 (Computer World Singapore)

...(CTO) Monday entered into an agreement with the International **Cyber Security** Protection Alliance (ICSPA) to work together to strengthen cybersecurity...

Fruity Instagram spam dies quickly on the vine

07/02/2013 21:49 (Computerworld Malaysia)

...to a phoney BBC page promoting weight-loss coffee. The page was clean of **malware** and doesn't appear to have posed a danger to the 35,000 or so...

Ubisoft breached, user account credentials compromised

07/02/2013 16:50 (Help Net Security)

...password on those, as well. I would add: beware of **phishing** attempts masked as emails from Ubisoft, asking for your personal or financial info,

Cybersecurity training on the rise for young students

07/02/2013 16:13 (The Leaf Chronicle)

...career in cybersecurity.) Amid rising sentiment that America's **cyber security** threat fully rivals the terrorism threat, it is becoming time for...

Current cybercrime market is all about Cybercrime-as-a-Service

07/02/2013 15:15 (Help Net Security)

...Crimeware-as-a-Service system includes developers selling exploits, **malware**, spyware, bots, spamming tools, tools for obfuscating the malicious...

Medical devices vulnerable to hackers warns FDA

07/02/2013 12:17 (SecurityInfoWatch.com)

including: Network-connected medical devices infected or disabled by **malware**; The presence of **malware** on hospital computers, smartphones and...

The father of Stuxnet may be the leaker of Stuxnet

07/02/2013 10:33 (Infosecurity)

The father of **Stuxnet** may be the leaker of **Stuxnet** Retired Marine Gen. James 'Hoss' Cartwright, the former vice chairman of the Joint Chiefs...

Keep all your software up-to-date with F-Secure

07/02/2013 09:42 (Help Net Security)

...victims machines, they can gain access to the machine, infecting it with **malware** that spies on the user and steals data. Barely a week goes by...

Litecoin-stealing Trojan found

07/02/2013 09:05 (Help Net Security)

...out there. As interest in and use of other ones rises, **malware** that tries to steal particular types of currencies from users' digital wallets...

Protect Android devices from theft and malware

07/02/2013 06:58 (Help Net Security)

Protect Android devices from theft and **malware** The new Norton Mobile Security with antivirus protects your Android phones and tablets from theft,

Guest View: Matching protection criteria to the next wave of threats

07/02/2013 06:51 (Computerworld Malaysia)

...rootkits. Today we find ourselves combatting the latest wave - advanced **malware**, targeted attacks and advanced persistent threats (APTs). While...

Telstra to provide Secure Internet Gateway technology to 11 Government agencies

07/05/2013 05:35 (Technology News)

...access to web services while protecting against internet threats including **malware** and hacking attacks. Paul Geason, Group Managing Director,

Windows to Go: Revolutionizing Malware Protection

07/05/2013 04:09 (Technology News)

Windows to Go: Revolutionizing **Malware** Protection (PR Web Via Acquire Media NewsEdge) Dallas, Texas (PRWEB) July 05, 2013 idcloak Technologies...

China, US to discuss cyber-security at forum

07/05/2013 02:36 (Digital Journal)

FireEye Reveals Key Characteristics to Identify Origin of Advanced Cyber Attacks

07/05/2013 00:52 (Technology News)

..."Comment Crew," previously linked to targeted attacks against the U.S. **government**. "In today's cyber threat landscape, identifying your enemy is a...

Courion to Present on the Future of Identity and Access Management at Cloud Identity Summit 2013

07/05/2013 00:52 (Technology News)

...identity and access management (IAM) technology and how the rise in **security** breaches and **cyber** risk are driving the next generation of IAM needs.

Cyber security at U.S. ports is insufficient, study says

07/05/2013 00:00 (Richmond Times-Dispatch (AP))

Cyber security at U.S. ports is insufficient, study says America s largest commercial ports have failed to shore up defenses against potential...

Financial Industry Is Serious About Cybersecurity

07/04/2013 20:08 (Bloomberg)

...exercise called Quantum Dawn 2 on July 18. This exercise will simulate a **cyber-attack** on the U.S. financial system. It will force individual...

EU adopts stricter penalties for cyber criminals

07/04/2013 17:25 (Help Net Security)

...police and judicial cooperation in this field. In the event of a **cyber attack**, EU countries will have to respond to urgent requests for help...

99 Percent Of All Android Installations Are Vulnerable To Hacking And Even Complete Takeover Of The Device

07/04/2013 12:41 (Forbes)

...a vulnerability in Android s security model that allows a **hacker** to modify APK code without breaking an application s cryptographic signature,

Trojanized Android app collects info, comments on NSA surveillance

07/04/2013 11:23 (Help Net Security)

...furiously in the background: it tries to download and install additional **malware** and attempts to send device info to a remote server each time...

Darkleech now delivering ransomware

07/04/2013 11:02 (Infosecurity)

...Chapro, was discussed by ESET last December. Now the anti-**malware** company has put some figures and details to a specific Darkleech campaign (which...

Fake Pinterest "Password changed" email leads to malware

07/04/2013 10:12 (Help Net Security)

Fake Pinterest "Password changed" email leads to **malware** Pinterest users beware: an email purportedly coming from the popular pinboard-style...

EMC Assigned Patent for Malware Detection Using Risk Analysis Based on File System and Network Activity

07/04/2013 07:14 (Technology News)

EMC Assigned Patent for **Malware** Detection Using Risk Analysis Based on File System and Network Activity (Targeted News Service Via Acquire Media...

FBI Warns of Increase in Spear-Phishing Attacks

07/04/2013 07:09 (Technology News)

FBI Warns of Increase in Spear-**Phishing** Attacks Jul 04, 2013 (M2 PRESSWIRE via COMTEX) -- Last week the FBI issued a warning about an increase...

CPC official urges global cooperation against cyber crimes, faster steps on norm

07/04/2013 04:31 (Technology News)

...enhance cooperation and bear the responsibilities together in the face of **cyber security** threats and challenges, he said. He urged the international...

News in review: has PRISM made the cloud unsafe?

07/08/2013 05:42 (Computer World Singapore)

...a spy tool, while a vulnerability was found that allows **malware** authors to modify Android apps without breaking their digital signatures - which...

Ultra Electronics to launch EnergyGuard

07/08/2013 04:26 (Help Net Security)

...protection solution, EnergyGuard, at October s Oil & Gas ICS **Cyber Security** Forum. EnergyGuard is designed to protect the devices at the critical...

Studies show cyberspying targeted US military, South Korea

07/08/2013 03:25 (Stars and Stripes)

...said those responsible for the spying had infected computers by "**spear phishing**" - targeted attacks that tricexpek users into giving up sensitive...

DoD's revised cyber policy to shift toward governmentwide standards

07/08/2013 02:00 (FederalNewsRadio.com)

...making. Where procedures and best practices are applicable to the whole **government**, it's working with the National Institute of Standards and...

Center for Internet Security to Expand Membership Options

07/08/2013 01:52 (Technology News)

...Internet Security, a nonprofit organization focused on enhancing the **cyber security** readiness and response of public and private sector entities,

EDA's overreaction to cyber attack highlights every agency's challenge

07/08/2013 01:34 (FederalNewsRadio.com)

EDA's overreaction to **cyber attack** highlights every agency's challenge The Commerce Department's Economic Development Administration spent almost...

Surviving a cyberwar depends on the target, experts say

07/07/2013 23:16 (Computerworld Malaysia)

...target, experts say The security community agrees it's important to protect **critical infrastructure**, but it's not clear which sectors are critical.

Don't ignore digital 'Cassandras' on security threat: Kaspersky

07/07/2013 23:16 (Computerworld Malaysia)

Don't ignore **digital** 'Cassandras' on **security** threat: Kaspersky That message continues to resonate as ever smarter **malware** authors show frighteningly...

Brazil expresses concern, seeks US clarification at reports of NSA spying on Brazilians

07/07/2013 16:30 (Pendleton Times-Post)

...that Internet users could shun operations that use U.S.-based **computer** servers to avoid **security** worries. France's Interior Minister used a July...

Maxis partners Symantec to offer Android mobile security

07/07/2013 00:15 (Computer World Singapore)

...(US$0.94) a month with features that include: - Anti-**Phishing** Web Protection - Through this feature, users are protected from malicious websites that...

Pwnium hacking contest winners exploited 16 chrome zero-days - RFID Laundry Tags Manufacturer

07/06/2013 14:18 (Amazines)

...in the other -- was dramatically more than the averageattack. The **Stuxnet** worm of 2010, called "groundbreaking" by someanalysts, used just four...

Anonymous attacks the Hawthorn Police Department

07/06/2013 12:53 (Democratic Underground)

...attacks the Hawthorn Police Department HAWTHORN, CA A team of **computer forensics** officers, and city information technology specialists, are still...

Android vulnerability allows attackers to turn apps into Trojans without breaking their signatures [Global Data Point]

07/06/2013 10:34 (Technology News)

...has existed in Android for the past four years can allow **hackers** to modify any legitimate and digitally signed application in order to transform...

Picky spyware ranks sensitive military documents

07/09/2013 01:17 (Computer World Singapore)

...where their computers would be attacked or by sending potential targets **spear-phishing** emails. When the **malware** successfully infected a computer,

Snowden revelations hover over US-China talks

07/09/2013 00:46 (Computer World Singapore)

...private intellectual property (IP) from US companies and research centres. **Cyber security** is at the centre of high-level meetings between the two...

Snowden affair blunts U.S. push for China to curb cyber theft

07/08/2013 22:57 (CTnow.com)

...intellectual property (IP) from U.S. companies and research centers. **Cyber security** is at the center of high-level talks between the two countries in...

Kaspersky, Trend Micro gain perfect scores in real-world protection test

07/08/2013 22:33 (Computerworld Malaysia)

...Antivirus 8.0, BitDefender Internet Security 2013, Emsisoft Anti-**Malware** 2013, F-Secure Internet Security 2013, and Fortinet FortiClient Lite...

5 security bolstering strategies that won't break the bank

07/08/2013 21:50 (Computerworld Malaysia)

...incident in the past year, ranging from malicious apps downloaded to a **mobile device** to unsecure Wi-Fi connections to lack of **security** patches from...

Fake Antivirus: 'System Doctor 2014'

07/08/2013 18:36 (Isssource.com)

...threats identified by System Doctor 2014 are from Microsoft s **malware** encyclopedia. Researches did say there were some similarities between the...

Middle East Espionage Malware is a RAT

07/08/2013 18:34 (Isssource.com)

Middle East Espionage **Malware** is a RAT Government agencies, telecom and energy organizations in the Middle East are the target of espionage **malware**...

Snowden: US And Israel Did Create Stuxnet Attack Code

07/08/2013 15:29 (Democratic Underground)

Snowden: US And Israel Did Create **Stuxnet** Attack Code NSA whistleblower Edward Snowden has confirmed that the **Stuxnet malware** used to attack...

Attack on South Korean targets part of a larger cyber-espionage campaign

07/08/2013 15:26 (Infosecurity)

...Korean targets part of a larger cyber-espionage campaign The March 20 **cyber-attack** on South Korean financial services and media firms, known as...

Ex-FBI chief: Intelligence community must do a better job of analyzing cyber threat landscape

07/08/2013 14:43 (SecurityInfoWatch.com)

...shouldn't be lulled into complacency just because hackers' attacks on **government** and business targets to date hadn't directly killed anybody. "There's...

South Korea Cyber Attacks Remain a Mystery

07/08/2013 14:11 (CIO Today)

...by the South Korean military. After years of reconnaissance and **spear**-fishing attacks, the attackers finally have enough information to draw...

McAfee displays how cyber attack works

07/08/2013 13:12 (Columbia Missourian)

McAfee displays how **cyber attack** works The anatomy of a **cyber attack** is displayed at the McAfee headquarters in Santa Clara, Calif., on Wednesday.

London Olympics cyber attack fears

07/08/2013 12:06 (Help Net Security)

London Olympics **cyber attack** fears The BBC has released details from 2012 Olympic Games officials about fears that the opening ceremony might...

Microsoft settles 3,265 software piracy cases in US and abroad; Company makes continued progress in commitment to protecting its intellectual property

07/10/2013 06:05 (Technology News)

...450,000 customers who reported counterfeit software, which was often riddled with **malware** and viruses or did not work as they expected. Among the...

SKorean cyber attacks tip of the iceberg: McAfee

07/10/2013 05:56 (Computer World Singapore)

SKorean cyber attacks tip of the iceberg: McAfee The anatomy of a **cyber attack** is displayed at the McAfee headquarters in California. Photo: AP...

U.S. Security Chief Sees Danger in Israel's Cisco Digital Plan

07/10/2013 05:11 (Bloomberg)

(CSCO) to turn the country digital with a super-fast fiber-optic **network** may **compromise** national security if precautions aren t taken, a U.S.

Cyber security collaboration in Europe

07/10/2013 04:58 (Help Net Security)

Cyber security collaboration in Europe The EU agency ENISA is supporting the development of standards for products and services in **cyber security**...

Microsoft reports hackings linked to report by Google researcher [Financial Mirror (Cyprus)]

07/10/2013 04:33 (Technology News)

...had launched "targeted attacks," a term generally used by **security** experts to refer to **cyber** attacks on corporate or government targets, with...

China, U.S. discuss cyber security

07/10/2013 02:56 (Technology News)

China, U.S. discuss **cyber security** WASHINGTON, Jul 10, 2013 (Xinhua via COMTEX) -- China and the United States held a strategic security dialogue...

Agency destroys $170K worth of IT gear over non-existent malware threat

07/10/2013 02:00 (Computerworld)

Agency destroys $170K worth of IT gear over non-existent **malware** threat Another $3 million worth of equipment at the Economic Development Administration...

China, U.S. talks on cyber security go well - Xinhua

07/10/2013 01:49 (Yahoo! News Canada)

NIST seeks input on cybersecurity framework

07/09/2013 23:56 (Computerworld Malaysia)

the NIST-developed framework represents the first time the federal **government** has sought to prescribe a wide-ranging approach to protecting critical...

Cryptocat vulnerability excuse sparks debate over open source

07/09/2013 23:14 (Computerworld Malaysia)

...can and wants them," said Murray Jennex, associate professor for **computer security** at San Diego State University. Dan Olds, an analyst for Gabriel...

Proof-of-concept exploit available for Android app signature check vulnerability

07/09/2013 22:41 (Computerworld Malaysia)

...channel," Oliva Fora said. The vulnerability presents benefits for Android **malware** authors because it allows them to add malicious code to legitimate...

Android Master Key Open to Attack

07/09/2013 18:54 (Isssource.com)

...a vulnerability in Android s security model that allows a **hacker** to modify APK code without breaking an application s cryptographic signature,

New Browser Exploit Kit Available

07/09/2013 18:23 (Isssource.com)

Windows Vista and even Windows 8, said a security researcher named Kafeine of **Malware** Don t Need Coffee. As far as the browsers go, Opera and...

2.5 million Californians exposed to identity theft in 2012

07/09/2013 16:29 (Infosecurity)

RAT Upgrade Targets Governments

07/09/2013 16:25 (Isssource.com)

RAT Upgrade Targets Governments A **spear phishing** campaign focused on government agencies in the U.S., Canada, Australia, a few European countries...

British defence giant hit by wave of cyber attacks

07/09/2013 13:17 (Technology News)

British defence giant hit by wave of **cyber** attacks Jul 07, 2013 (Financial Mail on Sunday - McClatchy-Tribune Information Services via COMTEX)

Free online virus scan from BullGuard

07/11/2013 03:21 (Help Net Security)

...their browser and in under a minute, it uses its anti-**malware** technology to check their system for potential threats and ensure that the current...

Business users visit most malicious websites, security academics find

07/10/2013 23:56 (Computerworld Malaysia)

...Interestingly, many of the hosts were unaware of their infection with **malware**. Business users account for 57 per cent of malicious attacks while...

Australia attracting 'significant' volume of Web threats: report

07/10/2013 23:24 (Computer World Singapore)

...allowed researchers to apply large scale analytics techniques to analyse **malware** sensor data. "Though Australia is geographically isolated in...

Economic impact of cyber espionage and IP theft hits U.S. businesses hard

07/10/2013 22:57 (Computerworld Malaysia)

Economic impact of **cyber** espionage and IP theft hits U.S. businesses hard Amid a week of economic meetings between top U.S. and Chinese officials,

Smart card readers for the iPhone and iPad

07/10/2013 21:40 (Computer World Singapore)

...including the CAC (Common Access Card) used by the U.S. military and **DOD** (**Department of Defense**). I tested the products by using an iPhone 4S and an...

Microsoft's new app security rules dubbed a paper tiger

07/10/2013 21:31 (Computerworld Malaysia)

...when an app has a serious vulnerability that cybercriminals are exploiting with **malware**. There is no timeline for fixes and no threats of having...

U.S.-China talks cover cyber issues, currency, Chinese reform

07/10/2013 19:06 (Yahoo! News Canada)

Biden Urges China to Stop Cyber Theft

07/10/2013 16:47 (Hawaii Reporter)

...discussions have created working groups to investigate issues including **cyber security** and climate change. Chinese state media reported Wednesday...

12 trends in privacy and security

07/10/2013 15:51 (Help Net Security)

...business naiveté. Corporations continue their delusional belief that data **security** and **cyber** privacy are a byproduct of purchasing better technology.

Facebook scam packs double whammy

07/10/2013 15:44 (Help Net Security)

Facebook scam packs double whammy A new **phishing** / **malware** delivery scam is doing rounds on Facebook, warns ThreatTrack's Chris Boyd. The lure...

ID Theft Affects 10% of Children

07/10/2013 14:45 (Infosecurity)

NATO cyber defense center fights tide of hacking attempts

07/10/2013 12:34 (Yahoo! Canada Finance)

7 reasons for security awareness failure

07/10/2013 12:12 (Computerworld)

...CBT, many companies have begun to incorporate social engineering or **phishing** simulations to their awareness programs. While there is nothing wrong...

Microsoft Fills 34 Holes

07/10/2013 11:41 (Isssource.com)

...critical font processing issue that allows attackers to infect systems with **malware**. The library is part of quite a few Microsoft applications,

Hunting for 'Whales' Using Targeted Malware

07/10/2013 10:30 (Enterprise Efficiency)

...or two. These targeted **malware** campaigns -- also referred to as **spear phishing** -- are designed to go after a specific person or organization.

Kremlin turns back to typewriters to avoid cyber leaks exposed by Edward Snowden

07/12/2013 04:09 (Computer World Singapore)

...to avoid cyber leaks exposed by Edward Snowden The future of high tech **cyber security** at the Kremlin... a typewriter. A Russian state service...

Mobile Threats to Your Online Security Are Skyrocketing

07/12/2013 02:29 (Private WiFi)

...mobile devices, according to a recent report from the Anti-**Phishing** Working Group (APWG) called In Mobile Threats and the Underground Marketplace.

Infographic: Is your information safe?

07/12/2013 01:38 (Help Net Security)

No one is immune to identity theft

07/12/2013 00:00 (Floyd County Times)

...numbers by using special storage devise when processing your card. **Phishing**. They pretend to be financial institutions or companies and send...

Foreign messaging services complicate government spying

07/11/2013 22:14 (Computerworld Malaysia)

...Bureau of Investigation bug the phones or houses of suspects or plant **malware** in their computers, Green said. As important as the encryption...

Dropbox, WordPress used in cyberespionage campaign

07/11/2013 21:51 (Computerworld Malaysia)

...The New York Times have added Dropbox and WordPress to their bag of **spear-phishing** tricks. The gang, known in security circles as the DNSCalc...

Oil and gas industry urged to focus on cybersecurity

07/11/2013 17:06 (Mywesttexas.com)

...cybersecurity capabilities and prioritize their actions and investments to improve **security**. "As **cyber** threats continue to increase in frequency...

LOREX releases new cloud-enabled connectivity solution

07/11/2013 13:54 (Technology News)

...release of Stratus Connectivity, which brings cloud-connectivity to **security digital** video recorders. Serving as the connectivity layer for all...

Nations Are Hiring Cybermercenaries, British Report Says

07/11/2013 12:36 (CIO Today)

...An annual report published by Britain's Intelligence and **Security** Committee says skilled **cyber** professionals are being hired by other nations,

Emergency Alert System vulnerable to hacking, report says

07/11/2013 12:32 (WJLA.com)

Emergency Alert **System vulnerable** to hacking, report says The Emergency Alert System, the vital service that interrupts television and radio...

Bit9 CEO: Trust-based model the new weapon in war against malware

07/11/2013 08:19 (Computerworld)

Bit9 CEO: Trust-based model the new weapon in war against **malware** CSO - Bit9 thinks you're fighting a new war using old weapons. The Waltham,

SaaS enhanced mobile device security

07/11/2013 08:00 (Help Net Security)

SaaS enhanced **mobile device security** Sophos announced Sophos Mobile Control 3.5, the latest version of its mobile device management (MDM) solution.

Who is winning the war on cybercrime?

07/15/2013 02:55 (Computerworld Malaysia)

Who is winning the war on **cybercrime**? A banking **trojan** - malicious software - has been installed to hijack bank transfers across Australia. A...

New Trend Micro solution targets data centres in AP

07/15/2013 00:48 (Computer World Singapore)

...virtualisation or cloud computing environments. Deep Security includes anti-**malware**, web reputation, firewall, intrusion prevention, integrity monitoring...

The ban on feds at Defcon draws a mixed reaction

07/14/2013 22:56 (Computerworld Malaysia)

...at Defcon draws a mixed reaction Call for U.S. **government** workers to avoid **security** conference rankles some **cyber** warriors, gets cheers from...

Targeted attacks exploit now-patched Windows bug revealed by Google engineer

07/14/2013 22:33 (Computer World Singapore)

...discussed was theoretically a critical flaw that hackers could use to plant **malware** on Windows PCs without users' knowledge, but asserted that most...

Enterprise anti-virus software test puts Kaspersky software out front, Microsoft at bottom

07/14/2013 21:39 (Computerworld Malaysia)

...important" but "is not a panacea" for security problems related to **malware**. "The tests showed that even with a relatively small sample set of...

Mobile malware, mainly aimed at Android devices, jumps 614% in a year

07/14/2013 21:27 (Computerworld Malaysia)

Mobile **malware**, mainly aimed at Android devices, jumps 614% in a year The threat to corporate data continues to grow as Android devices come...

Targeted malware attacks: What are they and how to defend against them (Photos)

07/14/2013 21:25 (Examiner.com - Ohio)

Targeted **malware** attacks: What are they and how to defend against them (Photos) Targeted **malware** attacks are on the rise in the past six months.

ARM building forensic skills of AccessData partners

07/14/2013 13:48 (Tech Channel MEA)

...added distributor ARM has entered the region building awareness of **digital forensics** amongst end users and skills capability of channel partners.

FBI Warns Public That Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks

07/14/2013 13:36 (Imperial Valley News)

FBI Warns Public That Cyber Criminals Continue to Use Spear-**Phishing** Attacks to **Compromise Computer** Networks San Diego, California - The FBI...

Cyberattack false alarm costs agency $3 million

07/14/2013 03:00 (The Journal Gazette)

...nothing of the sort. The disruption turned out to be a common **malware** infection on six computers that could have been erased with anti-virus...

Cyber security camp highlights national shortage

07/12/2013 20:40 (WDELL 1150AM - News Talk Radio)

Cyber security camp highlights national shortage Video player now loading; please wait... Students from Delaware universities learn how to hack...

Interview: Microsoft's Scott Charney

07/16/2013 04:26 (Infosecurity)

...DC, where he went to Main Justice to give legal advice to **government** and practice general litigation. Charney says his career path then took a...

Malware campaign strikes Asian, European governments

07/16/2013 04:22 (Computerworld Malaysia)

Malware campaign strikes Asian, European governments Trend Micro said that the attack emails purported to come from China's defense ministry...

BLOG: Can you hear me now? Yeah, hacked Verizon device can nab your texts and photos too

07/16/2013 04:11 (Computer World Singapore)

...Wireless released the Linux software update "that prevents its **network** extenders from being **compromised** in the manner reported by Ritter and...

South Korea blames North Korea for cyberattack - Timesonline.com: Technology

07/16/2013 03:08 (Timesonline.com)

...Korea. Researchers at Santa Clara, California-based McAfee Labs said the **malware** was designed to find and upload information referring to U.S. forces...

Unusual file-infecting malware steals FTP credentials, researchers say

07/15/2013 23:44 (Computerworld Malaysia)

Unusual file-infecting **malware** steals FTP credentials, researchers say About 70 percent of computers infected with this threat are in the US,

Cell phone amplifiers can be hacked

07/15/2013 23:07 (SFGate)

...issue being demonstrated by iSEC Partners. "The fix prevents the **network** extender from being **compromised** in the same manner." The news comes...

How keylogging malware steals your information (includes video)

07/15/2013 22:52 (Computer World Singapore)

How keylogging **malware** steals your information (includes video) Keyloggers are a malicious form of software that can secretly install on your...

Start-ups lean hard on CPU-based security technology to protect virtual environments

07/15/2013 22:52 (Computer World Singapore)

...the CPU for security. Bromium has a desktop anti-**malware** protection approach based on a specialized security-oriented hypervisor that relies...

Shadowlock ransom Trojan demands victims fill in survey for unlock key

07/15/2013 22:21 (Computer World Singapore)

...open the CD tray or open Windows utilities. "It turns out the **malware** author has a sense of humor," wrote Symantec researcher, Fred Gutierrez...

Chinese APT Worked through Cloud

07/15/2013 16:27 (Isssource.com)

...installed on the targeted computer in an effort to drop a piece of **malware**. To avoid raising any suspicion, a legitimate document displays. Once...

Mac spyware hides file extensions to evade detection

07/15/2013 15:53 (Infosecurity)

...spyware hides file extensions to evade detection A new cyber-espionage **malware** targeting the Mac operating system has been spotted, dubbed Janicab.

Cyber Security Diagnostic Tool

07/15/2013 15:15 (Isssource.com)

Cyber Security Diagnostic Tool Manufacturers often do not have a true **cyber security** plan because they just don t know where to start. Manufacturers...

DISA cloud contractors face strict security standards

07/15/2013 13:15 (Federal Times)

...have gone through the FedRAMP certification process: Hewlett-Packard, **Lockheed Martin**, Amazon Web Services, CGI and Autonomic Resources. At an...

Goofing off at Work Can Lead to Malware Infections and Data Breaches

07/15/2013 12:28 (Infosecurity)

Goofing off at Work Can Lead to **Malware** Infections and Data Breaches Surveys show that employees spend up to 30% of their working hours on private...

Governments are Big Buyers of Zero-Day Flaws

07/15/2013 09:56 (Infosecurity)

...zero-day flaws. "On the tiny Mediterranean island of Malta, two Italian **hackers** have been searching for bugs... secret flaws in computer code that...

Lloyds: Cybersecurity is the No. 3 Global Business Threat

07/15/2013 09:39 (Infosecurity)

...forensic analysis more difficult, and can be used to install new **malware** to evade detection and open more doors. In addition, privileged account...

Chinese hackers hurt business, Congressional committee told

07/15/2013 04:24 (Computer World Singapore)

...from tech companies and other U.S. businesses. "From **defense contractors** to manufacturing, no American company has been immune from the scourge...

As cyber attacks detonate, banks gird for battle

07/17/2013 04:04 (Lompoc Record (AP))

...SIFMA. About 50 banks and organizations will participate, including **government** agencies like the Treasury, the Department of Homeland Security,

Google releases a security patch for Android devices

07/17/2013 03:55 (Technology News)

...about the platform's open and free nature that can easily be a threat to **malware** and virus attacks. Jul 17, 2013 (M2 PRESSWIRE via COMTEX) --

Banks join cyber drill as attack risk grows

07/17/2013 03:00 (The Journal Gazette)

Banks join **cyber** drill as **attack** risk grows It s a war game, Wall Street style. It s a war game, Wall Street style. Banks large and small are...

Universities emerge as key hacking target

07/17/2013 03:00 (The Sacramento Bee)

...the University of Wisconsin said that when he set out to overhaul **computer security** recently, he was stunned by the sheer volume of hacking attempts.

ACMA issues ransomware warning

07/17/2013 02:49 (Computer World Australia)

...the fee must be paid and a payment portal. 16.5k **malware** infections reported daily in Australia Australians fleeced out of $93 million in 2012:

Cyber-sex trafficking: A 21st century scourge

07/17/2013 02:34 (KTXS.com)

...mother's cyber-sex operation, Delia is now under the care of a **government**-run temporary shelter for abused young girls and spoke to CNN in the company...

Almost half of world's stock markets targeted by cyber attackers last year: Study

07/17/2013 02:13 (Knoxville Times)

...A recent survey has revealed that almost half of the world's **security** exchanges were targeted by **cyber** attacks last year. A recent survey has...

New digitally signed Mac malware confuses users with right-to-left file name tricks

07/17/2013 01:20 (Computerworld Malaysia)

New digitally signed Mac **malware** confuses users with right-to-left file name tricks A new piece of digitally signed spyware for Mac OS X uses...

Signed Macintosh malware uses Right-to-Left Override

07/16/2013 23:42 (Computerworld Malaysia)

Signed Macintosh **malware** uses Right-to-Left Override **Malware** targeting OS X is using a technique called Right-to-Left Override in order to spoof...

Windows 8.1 steps up security with biometrics, encryption, and more

07/16/2013 23:42 (Computerworld Malaysia)

...Windows 8.1 Preview promises a safer experience, from antivirus and **malware** protections baked into IE 11, to VPN and remote-wiping enhancements...

New Android malware lowers the bar for cyberciminals

07/16/2013 23:42 (Computerworld Malaysia)

New Android **malware** lowers the bar for cyberciminals Discovery the latest example of a growing market in commoditized services for mobile like...

Android mega flaw fixed but phones remain vulnerable

07/16/2013 22:27 (Computerworld Malaysia)

...allows digital desperadoes to turn any legitimate application into a malicious **Trojan** been undetected in Android for four years, it seems to...

How to keep terrorists, hackers and other bad guys from stealing your data

07/16/2013 22:27 (Computerworld Malaysia)

...leak is also a somber reminder of the fragile nature of **computer security**. Even disregarding concerns over NSA surveillance, small businesses...

US retains spamming crown, Belarus inches toward the top spot, and three new countries enter into the "spam relaying" Dirty Dozen

07/16/2013 20:33 (Computer World Australia)

...indirectly these days, especially if it is overtly malevolent, such as: **Phishing** emails: These try to lure you into entering passwords into mock-ups...

Skype less of a threat than it seems

07/16/2013 19:53 (StarTribune.com)

...in full disclosure. The company warns that the application could allow **malware** to run up your phone bill, steal your information or erase your...

Police fight I.D. theft by arresting and informing

07/16/2013 19:46 (Connecticut Post)

...at helping businesses protect themselves from counterfeiting, skimming, and **network intrusion**, among other threats. "All types of businesses...

Cyber attacks on stock exchanges put markets at risk - report

07/16/2013 19:39 (Yahoo! News Canada)

Cyber-Attack Is a Systemic Risk, Exchange Study Says

07/16/2013 16:48 (Bloomberg)

Cyber-**Attack** Is a Systemic Risk, Exchange Study Says A significant number of exchanges have fought off sabotage via the Internet in the last...

Mac Malware Hides File Extension

07/16/2013 15:29 (Isssource.com)

Mac **Malware** Hides File Extension While out of the attack **malware** piece for quite awhile, there is now a piece of malicious software targeting...

APPetite for Information

07/16/2013 13:28 (Carnegie Mellon Today)

...with Sadeh, for instance, involved the reasons people fall for **phishing** scams, those fraudulent emails sent to uncover personal information. We...

Crime Scene Mapping technology

07/16/2013 13:23 (Wear ABC 3)

...minutes.. Once the data is collected it's then downloaded in a **computer** system bringing the accident or **crime** scene to life in 2 and three dimensional...

Cyber attacks on stock exchanges put markets at risk -report

07/16/2013 12:58 (Reuters.co.uk)

...interview. Among the exchanges surveyed, 53 percent said they experienced a **cyber attack** last year. The most common forms were Denial of Service attacks,

Cyber Attack Should Be Deemed Systemic Risk, Exchange Study Says

07/16/2013 11:53 (Washington Post - Bloomberg)

Cyber Attack Should Be Deemed Systemic Risk, Exchange Study Says July 16 (Bloomberg) -- A significant number of exchanges have fought off sabotage...

NIST proposes first federally funded cyber research center

07/16/2013 11:23 (FederalNewsRadio.com)

...look to the National Initiative for Cybersecurity Education, the federal **government**, universities and industry for help. "The FFRDC model is...

Acronis finds gaps in BYOD policy

07/18/2013 07:07 (Computerworld Malaysia)

...loss of confidential data, attack from hackers and threat from harmful **malware**. BYOD is a huge opportunity for companies, but it also brings...

Banks gird for cyber attacks

07/18/2013 01:08 (Philly.com)

Banks gird for **cyber** attacks It's a **war** game, Wall Street style. It's a war game, Wall Street style. Banks large and small are girding for an...

FBI Ransomware spotted on Mac OS X

07/17/2013 19:02 (Computerworld Malaysia)

security researchers warn, but add that the Mac version of the **malware** is technically different and much easier to remove. FBI Ransomware often...

Security company to release testing tool for SAP mobile access

07/17/2013 18:41 (Computerworld Malaysia)

...next month that tests if SAP systems have been correctly configured for **mobile device** use As SAP invests heavily in mobile, a **security** testing...

Decryption orders could violate human rights, Dutch judiciary council says

07/17/2013 18:41 (Computer World Singapore)

...Dutch government wants to introduce the decryption order because detection of **computer crime** is hampered by the use of encryption, especially in...

Apple browsers targeted by simple JavaScript ransom scam

07/17/2013 18:39 (Computer World Singapore)

Because the JavaScript is on the web page, there is no **malware** involved here. The same attack principle could be tried against Windows browsers...

Most BYOD businesses exposing data to cyber criminals

07/17/2013 18:39 (Computer World Singapore)

...confidential data, exposing it to theft, corruption, hackers, **malware** and more, according to security firm Acronis and independent research body...

Almost half of world's stock markets targeted by cyber attackers last year: Study

07/17/2013 17:49 (Albuquerque News.Net)

...A recent survey has revealed that almost half of the world's **security** exchanges were targeted by **cyber** attacks last year. A recent survey has...

Dirty AndroRAT: New Tool Lets Anyone Trojanize Android Apps

07/17/2013 15:51 (Infosecurity)

Dirty AndroRAT: New Tool Lets Anyone Trojanize Android Apps **Malware** authors are ever-adaptable, as evidenced by the rise of remote access tools...

Complex Coding Makes Web Apps a Bit Safer

07/17/2013 15:51 (Infosecurity)

Complex Coding Makes Web Apps a Bit Safer **Malware** and internet-based attacks continue to escalate in both volume and complexity, but when it...

Anonymous Hacked FEMA, Leaked Hundreds of Email Addresses

07/17/2013 15:46 (Motherboard)

Anonymous **Hacked** FEMA, Leaked Hundreds of Email Addresses Anonymous breached FEMA servers and pulled information on hundreds of agency contacts...

Four Busted for Hacking in Croatia

07/17/2013 13:51 (Isssource.com)

...against websites in Croatia, including ones belonging to the country s **government** and police are now under arrest. Four people suspected of being...

Ongoing Targeted Attack Takes Aim at Government Agencies in Europe and Asia

07/17/2013 13:11 (Infosecurity)

...agencies and large corporations are almost entirely dependent upon spear-**phishing** emails. While it may not be surprising that spear-**phishing**...

Cyberattackers Learn Targeted Advertising Tricks

07/17/2013 13:08 (CIO Today)

...with infections and scams. Cybergangs have been spreading infections by embedding **malware** in online ads, and paying for these malicious ads --

Comment: Secure Everything, Everywhere

07/17/2013 12:09 (Infosecurity)

increasingly struggle to defend themselves from the explosive growth in **security** threats and **cyber**-attacks. Without significant advances in security...

Quantum Dawn 2 will test Wall Street's cyber readiness

07/17/2013 11:26 (Computerworld)

...Decision-making Exercises -- Finance Sector (DECIDE-FS) from **Cyber** Strategies, a **security** services vendor based in Northfield, VT. DECIDE-FS...

Nasdaq forum website passwords hacked

07/19/2013 02:37 (Computer World Singapore)

Nasdaq forum website passwords hacked The **cyber**-**attack** happened on Tuesday, the same day a report was released saying that around half of the...

Quantum Dawn 2 will test Wall Street's cyber readiness

07/19/2013 02:35 (Computer World Singapore)

...Infrastructure Decision-making Exercises Finance Sector (DECIDE-FS) from **Cyber** Strategies, a **security** services vendor based in Northfield, VT. DECIDE-FS...

Bank security breaches destroy customer trust

07/19/2013 02:15 (Help Net Security)

...concerned about online banking fraud, according to Entersekt. Such fraud can include **phishing**, **malware**, man-in-the-browser and brute force attacks.

Attackers embedding backdoors into image files

07/18/2013 23:03 (Computer World Singapore)

...from the site. This is a curious steganographic way to hide the **malware**." Once the server is compromised, the attackers will modify the image's...

Singapore 12th top spam relaying country

07/18/2013 22:13 (Computerworld Malaysia)

...few timely and simple precautions to protect their people from hackers and **malware** attacks. Steps such as timely security patching, keeping up-to-date...

Fake emails on the rise, warns Telstra

07/18/2013 22:03 (Computer World Australia)

...hoax is where an email contains embedded links directing customers to a **phishing** website to gather personal details, Kane said. He added that...

Securities exchanges worry about major cyberattack as half report incidents

07/18/2013 21:44 (Computer World Singapore)

...sector to and severely damage investor confidence," said the author of **Cyber**-**crime**, securities, markets and systemic risk,Rohini Tendulkar. Although...

New Android RAT Malware

07/18/2013 17:48 (Isssource.com)

New Android RAT **Malware** Tools that can inject legitimate Android apps with open-source software that allows an attacker to control of a smartphone...

U.S. Tops Countries Sending Out Spam

07/18/2013 17:36 (Isssource.com)

...sends out indirectly these days. The type of spam sent out includes: **Phishing** emails: These try to lure you into entering passwords into mock-ups...

Cyber Security Assessment Service

07/18/2013 17:17 (Isssource.com)

Cyber Security Assessment Service Knowledge is king and sometimes manufacturers are totally lacking in any understanding of how poor their security...

Taiwan a "testing ground" for Chinese cyber army

07/18/2013 16:09 (Reuters.co.uk)

...networks. It followed another report in February by U.S. **computer security** company Mandiant that said a secretive Chinese military unit was probably...

How Does Cyber Warfare Work?

07/18/2013 12:58 (Forbes)

...something. In cyber warfare sabotage can be something as benign as dropping a **government** s website to causing a nuclear meltdown at a nuclear plant.It...

Apps exploiting Android “Master Key” bug offered on Google Play

07/18/2013 10:43 (Help Net Security)

...code of any app without breaking its cryptographic signature and pass **malware** off as legitimate apps. But even though both vulnerabilities have...

Wall Street Launches a Massive Cyber-Attack -- On Itself

07/18/2013 08:49 (Forbes)

Wall Street Launches a Massive **Cyber**-**Attack** -- On Itself Wall Street s largest trade group is about to try taking down the financial nerve center...

Malware market peddles tools to exploit Android infections

07/22/2013 05:18 (Computerworld Malaysia)

Malware market peddles tools to exploit Android infections Security firm Symantec reports availability of a tool that can infect legitimate Android...

U.A.E. Thwarts Cyber-Attack Attempts on Government Sites

07/22/2013 05:17 (Bloomberg)

U.A.E. Thwarts **Cyber**-**Attack** Attempts on **Government** Sites The United Arab Emirates, the second-largest economy in the Middle East, fought off...

Apple's developer website attacked, can't rule out stolen data

07/22/2013 04:02 (The Interlake Today)

Event Viewer scam still targeting Australians: Police

07/22/2013 00:49 (Computer World Australia)

...being warned to hang up on telemarketers who phone up and claim that their **computer** has a **virus**. The scam, known as Windows Event Viewer - or...

Cyber drills like Quantum Dawn 2 vital to security in financial sector

07/21/2013 23:58 (Computer World Singapore)

Cyber drills like Quantum Dawn 2 vital to **security** in financial sector **Cyber** exercises, like the Quantum Dawn 2 drill carried out by dozens of...

Encryption helps keep your personal information private

07/21/2013 23:43 (The Daily Texan)

...credit report regularly, don t reuse or share passwords and keep anti-**virus** software installed on your **computer**. If you want to be really safe,

Foreign VPNs raise the bar against US government spying

07/21/2013 22:38 (Computerworld Malaysia)

...terrorist activity. In addition, government agencies are capable of planting **malware** to collect data directly from a suspect's PC or gather phone...

Black Hat: Top 20 hack-attack tools

07/21/2013 22:04 (Computerworld Malaysia)

...to automate information gathering that can be used to make **spear phishing** messages more convincing by mimicking how individuals interact with...

Hackers breach Nasdaq community forum website

07/21/2013 22:01 (Computer World Singapore)

...should be more clear about the security risk posed, and warned over potential **phishing** attacks as a result of the breach. "What also irks me is...

Huawei says it 'shares the same cyber security goals' as the UK government

07/21/2013 22:01 (Computer World Singapore)

Huawei says it 'shares the same **cyber security** goals' as the UK **government** Chinese networking giant Huawei has said that it 'shares the same...

SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones

07/21/2013 09:37 (Forbes)

...Flaw Could Affect Millions Of Phones Smartphones are susceptible to **malware** and carriers have enabled NSA snooping, but the prevailing wisdom...

BBB: Don't get 'clickjacked' — you won't 'like' it

07/21/2013 06:23 (Odessa American Online (AP))

you could be activating a scam. Clickjacking starts like most online **phishing** scams. You receive an email, social media message or text that...

5 ways hackers attack you, and how to counter them

07/21/2013 02:20 (Sioux City Journal)

...counter their malicious acts. Here are five popular hacker strategies. **Phishing** scams Lucky you! A Nigerian prince has selected you to help smuggle...

Targeted Malware Attacks in Asia, Europe

07/19/2013 19:09 (Isssource.com)

Targeted **Malware** Attacks in Asia, Europe A targeted attack sent emails loaded with **malware** to representatives of 16 European countries and some...

Indonesia Joins China as Cyber-Attack Powerhouse

07/23/2013 00:29 (Bloomberg)

Indonesia Joins China as **Cyber**-**Attack** Powerhouse Indonesia isn't known as an epicenter for hacking, but the Southeast Asian country was the source...

Medical Device Hackers Find Government Ally to Pressure Industry

07/23/2013 00:29 (Bloomberg)

...to take remote control of the device. The diabetic and **computer security** researcher went public with his findings at a hacker conference after...

F5 data center firewall aces performance test

07/22/2013 22:35 (Computerworld Malaysia)

...network, IP-Intelligence can block traffic from botnets, Windows exploits, **phishing** exploits, and other classes of threats. IP-Intelligence is not enabled...

Cybercrime costs US economy up to $140 billion annually, report says

07/22/2013 22:25 (Idaho Statesman)

...report looked at intellectual property theft, cybercrimes such as **phishing** and text messaging fraud, loss of sensitive business information,

Fake emails on the rise, warns Telstra

07/22/2013 22:15 (Computer World Singapore)

...hoax is where an email contains embedded links directing customers to a **phishing** website to gather personal details," Kane said. He added that...

Researcher finds major encryption flaw in older mobile SIM cards

07/22/2013 22:15 (Computer World Singapore)

...possible to take control of a handset using a binary SMS text message to upload **malware**. This piggybacked on the carrier over-the-air (OTA) process...

Should you keep using Windows XP?

07/22/2013 21:32 (Computer World Singapore)

...become less and less secure. And it may not be all that gradual. **Malware** authors love to use outdated software as a path into your PC and the more...

The Real Cost of Cyber Crime

07/22/2013 19:06 (Bloomberg)

The Real Cost of **Cyber Crime** July 22 (Bloomberg) -- McAfee Chief Technology Officer Michael Fey discusses the dollar cost to the economy of **cyber**...

Backdoors Embedded into Image Files

07/22/2013 18:36 (Isssource.com)

...site, he said. This is a curious steganographic way to hide the **malware**. Once the server suffers compromise, the attackers will modify the image...

Google Glass Vulnerable to Attack

07/22/2013 18:19 (Isssource.com)

...Vulnerable to Attack Just after Google fixed one Wi-Fi **security** problem with its wearable **computer** Glass, researchers found another problem,

Interface weakness opens servers to attacks

07/22/2013 15:40 (IT World Canada)

Notre Dame seeing more cyber attacks

07/22/2013 13:13 (WSBT)

more and more frequently. David Seidl, director of information technology **security**, says **cyber** attacks happen at Notre Dame every day. A handful...

File Infector Malware Growing in U.S.

07/22/2013 12:52 (Isssource.com)

File Infector **Malware** Growing in U.S. New variants of the PE_EXPIRO family are out and while they do contain file infectors, but they also have...

5 hacking scams you should be aware of

07/22/2013 12:46 (HoumaToday.com)

...their malicious acts. Here are five popular hacker strategies. 1. **Phishing** scams Lucky you! A Nigerian prince has selected you to help smuggle...

Security Spending to Hit $46 Billion

07/22/2013 11:28 (Isssource.com)

Security Spending to Hit $46 Billion Digitization of **critical infrastructures** has provided substantial benefits in terms of improved productivity,

Passwords of 1.8M Ubuntu Forums users compromised in hack

07/22/2013 10:19 (Help Net Security)

...(she?) did it to harvest user information that can be used for spamming, account hijacking, **spear phishing** emails, and more. Follow @zeljkazorz

DHS gears up to unleash Einstein 3 to better secure federal networks

07/22/2013 08:25 (FederalNewsRadio.com)

...majority of the large agencies has signed up for a new tool in the **war** against **cyber** attacks. A majority of the large agencies has signed up for...

Week in review: Hijacking connected cars, Android backup flaw, help desk security threats

07/22/2013 06:53 (Help Net Security)

...police agencies in various participating countries to address emerging **digital crime** at the national and international level. Including expertise...

Mobile devices infected with malware

07/24/2013 03:31 (Computer World Singapore)

Mobile devices infected with **malware** More than 0.5 percent of mobile devices were infected with **malware**, according to the newly released Kindsight...

72% can't securely manage multiple computing environments

07/24/2013 03:12 (Help Net Security)

...opportunities created by multi-platform computing, enterprise mobility, and **cyber security**. For example, many Federal agencies are looking for solutions...

Singapore launches new Masterplan to enhance cyber security

07/24/2013 02:52 (Computerworld Malaysia)

Singapore launches new Masterplan to enhance **cyber security** The vision of the new five-year Masterplan is for Singapore to be a trusted and robust...

SIM card hack has severe implications for business

07/23/2013 22:59 (Computerworld Malaysia)

...will be presenting findings to that effect at the annual Black Hat **computer security** conference at the end of the month. The impact of hacked...

Hackers have new way to steal info from smart phones

07/23/2013 21:35 (CBS 5 AZ KPHO)

...data, e-mails and other personal information users like to keep private. But **cyber security** experts tell CBS-5 News, there's a new threat, not...

Cisco Deals for Security Provider

07/23/2013 19:03 (Isssource.com)

...Cisco Systems Inc. will pay $2.7 billion to pick up **cyber security** software provider Sourcefire Inc. In a move to boost its network security...

Spam Botnet Dodges Detection

07/23/2013 18:08 (Isssource.com)

...responsible for sending the spam, said researchers at Trend Micro. The **malware** victim gathers spam data such as backup mail server, sender name,

Cyber crime leads to job loss

07/23/2013 17:50 (Computerworld Malaysia)

Cyber crime leads to job loss 508,000 U.S. jobs lost as a result of malicious cyber activity, according to McAfee report. 508,000 U.S. jobs lost...

Global Cybercrime, Espionage Costs $100–$500 Billion Per Year

07/23/2013 15:54 (Infosecurity)

Global Cybercrime, Espionage Costs $100 $500 Billion Per Year **Cyber**-**crime** and espionage is clearly a costly scourge for businesses and governments,

UAE Fends Off Cyber-Attacks Originating in Egypt

07/23/2013 14:20 (Infosecurity)

which it said is plotting to overthrow the UAE s Western-backed **government** system. From the first moment of the attack, our approach was twofold,

Report: China Uses Taiwan as Test-Bed for US Cyber-Espionage Attacks

07/23/2013 13:47 (Infosecurity)

...new attacks being mounted against Taiwan are geared to use **spear phishing** email to initiate advanced persistent threats. Mails containing malicious...

Android spyware infections on the rise

07/23/2013 11:36 (Computerworld)

...infections on the rise About 1% of Android devices are infected with **malware**, according to Alcatel-Lucent's Kindsight Security Labs IDG News...

Cisco welcomes IDA's Cyber Security Masterplan

07/25/2013 03:13 (Computerworld Malaysia)

Cisco welcomes IDA s **Cyber Security** Masterplan The plan will reinforce Singapore s position as a global economic player, says Cisco MD for Singapore...

Don't be fooled by study's dramatically lower cyberthreat estimate, experts say

07/25/2013 02:10 (Computer World UK)

A company should then figure out the worst that can happen if a **network** is **compromised** by one of these adversaries. The study's macroeconomic...

Syrian Electronic Army hacks into Viber support website

07/24/2013 23:40 (Computer World Singapore)

...was defaced after a Viber employee unfortunately fell victim to an email **phishing** attack," a Viber Media spokesman said Wednesday via email.

Compromised websites at hosting companies more than doubling daily from a year ago, report finds

07/24/2013 23:40 (Computer World Singapore)

...the hacked websites they break into to post content such as porn and **malware**, for example, to draw in anyone who receives a spam message they...

Once more into the breach: How hackers compromise websites like Apple's

07/24/2013 23:40 (Computer World Singapore)

...than a day, you've probably been on the receiving end of a "**phishing**" email, which invites you to log on to a site that looks and feels like,

Cybercrime costing global economy up to $400 billion a year, says new estimate

07/24/2013 22:01 (Computerworld Malaysia)

business leaders and others struggle to get their arms around why **cyber security** matters, they need solid information on which to base their...

New Trojan could create headaches for banks, customers

07/24/2013 22:01 (Computerworld Malaysia)

...criminals are cheering on,' RSA said With the major developers of banking **malware** laying low, a new crook on the block has emerged gunning to be...

Cybercrime Costs U.S Economy $100 Billion and 500,000 Jobs

07/24/2013 22:01 (Computerworld Malaysia)

Cybercrime Costs U.S Economy $100 Billion and 500,000 Jobs A new economic model developed by the Center for Strategic and International Studies,

Citadel malware active on 20,000 PCs in Japan, says Trend Micro

07/24/2013 22:01 (Computerworld Malaysia)

Citadel **malware** active on 20,000 PCs in Japan, says Trend Micro The **malware**, which steals financial and login data, is actively sending data...

Malicious cyber activities caused financial and job losses around the globe

07/24/2013 19:44 (Examiner.com - Minnesota)

business leaders and others struggle to get their arms around why **cyber security** matters, they need solid information on which to base their...

Cyber-sabotage is way too easy

07/24/2013 18:20 (Sun Sentinel)

Cyber-sabotage is way too easy LONDON **Hacking** power plants and chemical factories is easy. LONDON **Hacking** power plants and chemical factories...

First agency set to use new DHS cybersecurity program

07/24/2013 17:02 (Federal Times)

...Einstein 3, the latest version of a Department of Homeland **Security** program designed to protect agency **computer** systems from cyberattacks, is...

Developing A Smarter BYOD Policy For You

07/24/2013 16:34 (Forbes)

...on your employer s approach to items such as company policies, **security**, reimbursement plan and use of **mobile device** management (MDM) software.

Introduction to Cyber-Warfare

07/24/2013 14:44 (Help Net Security)

...them. Naturally, they started with a chapter defining the idea of **cyber war**, and the issues of attribution, deception, and intelligence. The...

U.S. donates crime-fighting tools to Costa Rica

07/24/2013 12:19 (Technology News)

...assistance to local prosecutors through the program, in areas such as **cyber**-**crime**, international **crime** syndicates and victims' assistance programs.

SanDisk wireless storage drives excel; wearable MeCam a clunky camcorder

07/24/2013 12:19 (Computerworld)

...reached at kshaw@nww.com. Follow him on Twitter: @shawkeith. Read more about anti-**malware** in Network World's Anti-**malware** section. By Keith Shaw

Oxford Expands its Cybersecurity Education

07/24/2013 11:42 (Infosecurity)

...open the doors on a new Centre for Doctoral Training in **Cyber Security**. The center will train around sixteen advanced graduate students each...

iOS and Android VoIP Service Viber Hacked by Syrian Electronic Army

07/24/2013 11:05 (Infosecurity)

...occurred "after a Viber employee unfortunately fell victim to an email **phishing** attack. The **phishing** attack allowed access to two minor systems:

Move Over Zeus: KINS Banking Trojan Looks to Be the Next Great Financial Crimeware

07/24/2013 10:09 (Infosecurity)

Move Over Zeus: KINS Banking **Trojan** Looks to Be the Next Great Financial Crimeware A new professional-grade banking **trojan** is stepping into the...

Lakeland Kitchenware Hacked with Java 0-Day

07/24/2013 10:06 (Infosecurity)

...occurred it was Java. "Lakeland had been subjected to a sophisticated **cyber-attack** using a very recently identified flaw in the Java software used...

Smishing: A Serious Identity Theft Scheme

07/26/2013 06:01 (Mainstreet)

...their smartphones, but this information can be accessed by criminals through **phishing** and other scams. One example of a **phishing** scam is a criminal...

Oil, gas field sensors vulnerable to attack via radio waves

07/26/2013 05:49 (Computer World Singapore)

...research. Researchers Lucas Apa and Carlos Mario Penagos of IOActive, a **computer security** firm, say they've found a host of software vulnerabilities...

Five charged with stealing 160+ million credit card numbers

07/26/2013 05:20 (Help Net Security)

Once the network was infiltrated, the defendants placed malicious code, or **malware**, on the system. This **malware** created a back door, leaving...

McAfee teaches online safety to over 15,000 children in SEA

07/26/2013 05:16 (Computerworld Malaysia)

...the two main online threats. To further raise awareness on **cyber security**, McAfee held its second annual McAfee Global Community Service Day...

5 charged in largest U.S. hacking scam

07/26/2013 04:09 (The Daily Journal (AP))

...its computer network. About 800,000 card numbers were stolen in an **attack** on the Visa **network**, but the indictment did not cite any loss figure.

Five indicted in massive hacking scheme

07/26/2013 01:38 (Computer World UK)

...network. Once the network was infiltrated, the defendants allegedly placed **malware** on a network, creating a back door that allowed further access.

From cruise offers to banking Trojans, SMS spam clogs channels

07/25/2013 23:53 (Computerworld Malaysia)

As popular as free stuff scams are, they still placed behind **phishing** for bank accounts and adult content junk in spam volumes during the period.

SQL flaws remain an Achilles heel for IT security groups

07/25/2013 22:37 (Computerworld Malaysia)

the attackers rapidly escalated their privileges on the network to install **malware** and backdoors for stealing credit card and other data. Via...

Cybercriminals increasingly use the Tor network to control their botnets, researchers say

07/25/2013 20:44 (Computerworld Malaysia)

...botnets, researchers say Researchers from ESET discovered two new **malware** threats that use control servers within the Tor anonymity network.

Firms Lack Security Knowledge: Report

07/25/2013 18:54 (Isssource.com)

...Knowledge: Report There has been an uptick in more sophisticated and targeted **malware** attacks over the last 24 months, a new survey said. There...

C-Level Fears Own Security Profile

07/25/2013 18:23 (Isssource.com)

...(47 percent) said they are not making use of advanced **malware** analysis tools, according to the ThreatTrack Security report. The independent blind...

Bidding is Open for the DHS' $6 billion Security Hub

07/25/2013 17:28 (Infosecurity)

...Economic Development Administration s $3 million fight against non-existent **malware**. The DHS will act as the central management authority for the...

Most Organizations Don't Assess Time to Incident Detection as Key Security Metric

07/25/2013 16:48 (Infosecurity)

...example, among threat management metrics, the percentage of endpoints free of **malware** and viruses led with 38% of security managers citing it as a...

New Banking Trojan Found Underground

07/25/2013 15:47 (Isssource.com)

...to work its way through the ranks. This is the first actual commercial **Trojan** we ve seen in a while, since Citadel was taken off the market,

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

Are Your Privileged Passwords Out to Get You?

The rain beads on the windshield as Jeff moves slowly through the Dallas traffic. It is 7 p.m. and it has been a long week of planning for the upcoming IT reorganization. Jeff's phone starts to buzz on the passenger seat—it's Steve from SecOps. Strange time for a call. "Jeff, we are seeing some strange behavior on the domain controllers over in Austin. One of the monitors picked up a service being shut down but no one should be working on those boxes. We did some digging and found the connection is coming from a call center workstation in Dallas. But that's not all. Seems like there are some other strange things coming from the Austin data center now." Jeff sucks in his breath, "I'll be there in 20," and takes the next freeway exit.

The initial compromise came from malware delivered through a spear phishing attack on a call center workstation. The attacker then dumped memory looking for NTLM password hashes residing in memory. Unfortunately, a domain admin had been looking at the workstation due to a troubleshooting ticket a few days before. The NTLM password hash from memory was all that was needed to initiate a "Pass the Hash" attack directly to the domain controllers, impersonating the domain admin. From there, the attack escalated and the attacker jumped from server to server looking for intellectual property, installing backdoors and generally wreaking havoc. This resulted in many long nights for Jeff, Steve and the rest of the team. Containing the attack, remediating machines, removing access, and performing the necessary forensics went from days to weeks. The cost was huge.

"Pass the Hash" is a very easy means for attackers to gain further access even when using the latest Windows operating systems, security patches and out-of-the-box configuration. However, this attack can be easily prevented through effective management of the domain admin passwords. Regular password changing—ideally after the use of a domain admin account—mitigates the "Pass the Hash" attack by making the NTLM password hash useless since the password has been changed.

The IT security industry is finally coming around to the idea that perimeter security is insufficient. Best practice security principles like least privilege and defense-in-depth can help to reduce the number of workstation compromises and can also limit the damage when such compromises happen. Often, password practices are forgotten.

What can be done? Turn the page and find out…

1. Separate the administrator accounts into a regular AD account and a user-specific DA account for use only when privilege is needed.

2. Lock down the DA account passwords in a secure place where the administrator can get to it when needed.

3. Change the DA account password to a new random value after every usage.

These simple steps can dramatically reduce the risk of a site-wide attack in the case of a single breached workstation. While these steps can be done manually, they can also be automated with scripts or completely controlled using commercial password management software designed for IT admin teams.

There are other benefits that can be realized through effective management of privileged passwords, such as ensuring accountability across administrator teams, easier password rotation when staff turnover occurs, and the ability to meet auditor and compliance requirements.

About The Author

Jonathan Cogley is founder and CEO of Thycotic Software, a Washington D.C.-based security software company best known for Secret Server - enterprise password management software used by over 75,000 IT administrators in companies throughout the world.

To learn more about Thycotic Software, visit us online at http://www.thycotic.com/

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:

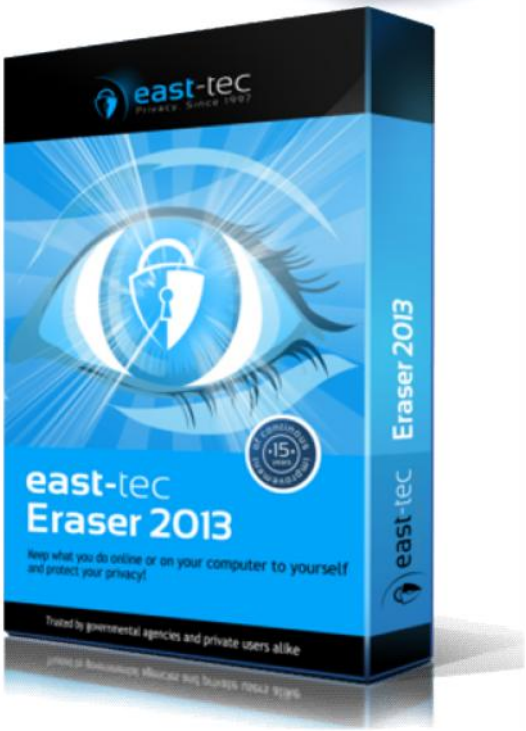
http://www.naisg.org/techtips.asp

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 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: 07/29/2013

CDM

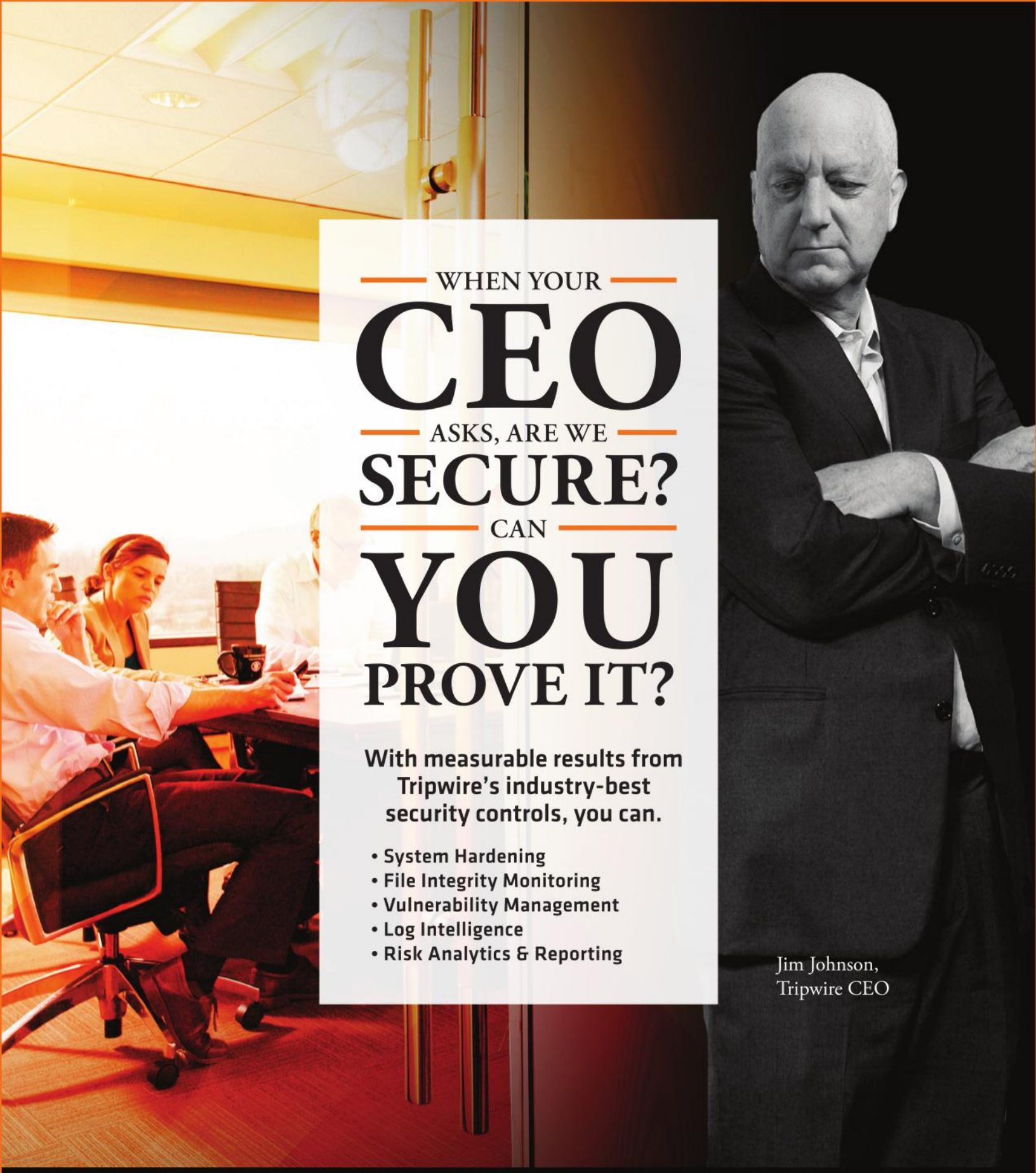
CYBER DEFENSE MAGAZINE

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/



WHEN YOUR

CEO

ASKS, ARE WE

SECURE?

CAN

YOU PROVE IT?

With measurable results from Tripwire's industry-best security controls, you can.

- System Hardening
- File Integrity Monitoring
- Vulnerability Management
- Log Intelligence
- Risk Analytics & Reporting

Jim Johnson,
Tripwire CEO

Tripwire is the leading provider of risk-based security and compliance management solutions, offering the broadest set of foundational security controls in the industry.
Visit www.tripwire.com

tripwire®
CONFIDENCE: SECURED