CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

NOVEMBER 2014

MORE INSIDE!

CONTENTS

Is the CyberGrinch about to Steal Your Cookies? 3

Lame Duck and Beyond: A Policy Outlook on the Incoming Congress 4

Modern Threats Signal Urgency for Security Strategies Overhaul 7

Threats are Doing Their Knock, Knock… Are We Cyber Safe for Real? 10

Recent Regulatory Focus on Cybersecurity Fuels Financial Controls 13

Q&A with Tim Clark, The FactPoint Group, on Automated Malware Removal 17

What is Data Security in the Cloud? 19

ForgeRock Delivers Solution to Help Government Agencies Accelerate Secure Rollout of Digital Services For Citizens 23

Web Server Security – Mind it before you hacked 27

Is it ethical to sell zero day exploits? 31

Unconventional Fraud 34

Assessing and Profiling the Insider Threats in Information Technology 38

DDoS Out in Full Force 43

The Anatomy of a Social Media Cyber Attack 45

How to Avoid Incorrectly Labeling Innocent Customers as Guilty this Holiday Shopping Season 47

Verizon's Supercookies and using a VPN as Defense 51

Top 3 Myths About Antivirus Software 53

NSA Spying Concerns? Learn Counterveillance 54

Top Twenty INFOSEC Open Sources 55

National Information Security Group Offers FREE Techtips 56

Job Opportunities 57

Free Monthly Cyber Warnings Via Email 57

Cyber Warnings Newsflash for November 2014 60

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

PierLuigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Robert B. Dix, Jr.
Simon Crosby
Milica Djekic
Joe Holman
Giorgio Bonuccelli
Daniel Raskin
Gunjan Tripathi
Steve Nowicki
Luis Corrons
Dr. Joshua Sinai
Evan Blair
Reed Taussig
Patrick Lincoln
Todd Weller

and many more…

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Is the CyberGrinch about to Steal Your Cookies?

As we work towards a wrapup of 2014 and peer forward into the 2015 horizon, I can't help but think about all of the Cybercrime going on today. Especially in the USA. Not to mention the dynamic shift now taking place whereby mobile banking and mobile commerce have become a reality. Instead of hopping into your car and driving to the local retail outlet, it's already on your smartphone, or tablet. Ecommerce has arrived in the form of Mcommerce – it's gone mobile. Banks are also finding it more convenient to deliver products and services from a mobile banking ATM experience to taking a loan application to even opening a new account remotely through mobile devices.

Today's threats far surpass the culmination of attacks that have taken place over more than a decade. We're truly in the early stages of cyberwarfare. Nation states attacking nation states every day and cyber criminals abound – looking for every opportunity to steal your identity like the cybergrinch stealing the cookies you left out for ol' St. Nick. Don't think this a daily barrage, just take a look at Norse's real-time attack map at http://map.ipviking.com – with honeypots around the globe, can you see what they see?

You can even buy Zero-day exploits – but do you have to be as big or powerful as Microsoft to pay for them and is it Ethical? This is one of the questions we tackle in this month's edition. So, yes, there's tons of attacks happening, lots of malware out there, some even for sale – will it ever end? Probably not. This means that there will, of course, be many many more INFOSEC professional jobs in 2015. This means that there will be new players on the block at RSA Conference 2015, like Norse, who is taking a more proactive approach to studying cyberwarfare attack patterns in real-time.

I expect 2015 to be a very exciting year - we'll see that www.privacyrights.org will hit a milestone of over over 1 billion personally identifyable information (PII) records stolen by the end of the year. Keep an eye on that website for the current breaches.

As you read through this November's edition of CDM, I hope you'll see why ever edition, I suggest you stay even more vigilant now, than ever. It's only getting worse. Through this barrage of cyberwarfare and cybercrime, there will be newfound opportunities for more creative and proactive information security startups to hit the scene, trying to help you get one step ahead of the next threat. Stay tuned in. Stay ever so vigilant.

Don't forget to keep an eye on the latest antivirus software tests at the Virus Bulletin's VB100: https://www.virusbtn.com/vb100/latest_comparative/index where you'll see some promising new entrants who realize that traditional methods can't stop the Cybergrinch. They include GData, one of our favorites – Emsisoft, as well as ULIS, Wontok, Kromtech and Avetix. The Cybergrinch will not be sleeping in this winter. He's out for your cyber-cookies. And if your cyber-cookies are mission critical data, consumer records, or anything else of importance, you better lock your cookie jar before he arrives!

To our faithful readers, Enjoy

Pierluigi Paganini

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

Lame Duck and Beyond: A Policy Outlook on the Incoming Congress

By Robert B. Dix, Jr.

The 2014 U.S. mid-term elections will produce a major shift of political power in our Nation's Capital. Republicans will control the U.S. Senate, its agenda, and committees. And in the House of Representative, the Republican majority has grown. This can either ease the long-running stalemate between the White House and Congress or aggravate it even more.

Republicans have an opportunity to demonstrate their ability to work on passing meaningful legislation that will make a difference for the American people and send it to the White House to sign… or not.

But, before the shift in power takes place in January, Democrats have a few months of Senate control remaining. This is a period of congressional transition known as the lame duck session to push forward with its agenda. What could the lame duck mean for cybersecurity and technology policy issues? It could mean a lot.

Cybersecurity policy, defense and communications policies, patent reform, and perhaps even corporate tax reform all stand to be impacted by revised political strategy and by changes in the leadership of congressional committees that oversee these issues. Below we explore the reverberations emanating from the elections and member retirements that will be seen through the lame duck session and beyond.

Cybersecurity

For several years, policymakers have attempted to advance legislative initiatives that are intended to address the growing risk environment in cyberspace. Improving the security of government networks and the partnership between the security industry and government to reduce cyber risks is a high priority. Legislation is necessary to improve bi-directional information sharing and collaboration between the private sector and government, but also could impact how network equipment is designed (such as the use of specific security controls and mandatory implementation of certain technology standards) and how/when cybersecurity incidents are reported.

The House has passed several cybersecurity bills pertaining to information sharing, cyber workforce development, and government computer security reform. The Senate, however, has passed no cybersecurity legislation. Why not?

This is largely because the Senate Democratic leadership has focused on passing a comprehensive bill that addresses many issues in one bill. A previously introduced bill included an expanded regulatory approach with static, costly, and compliance-based provisions that would have stymied innovation and was largely opposed by industry. The measure twice failed

to gain the necessary votes to pass. With the Senate shifting to Republican control next year, it is more likely that expanded regulation of privately -owned and -operated networks will be off the table and that Congress will consider a series of individual cyber bills that will move the needle in a positive direction and could be signed into law.

Intelligence and Defense

The one stumbling block for information sharing legislation, however, might be continuing concerns by privacy advocates, libertarians, and members of both sides of the aisle regarding NSA surveillance operations. It remains to be seen whether Congress might choose to address the issue as part of the "must pass" National Defense Authorization Act during the lame duck session.

Communications and Patent Reform

When the Senate does change hands, the Republican-led Congress will consider a major rewrite of the Communications Act, which empowers the FCC to regulate various sectors of the communications industry. Incoming Senate Commerce Chair John Thune (R-SD) pledged to join his House Republican counterparts as they undertake a years-long process to rewrite and update the country's telecommunications laws to reflect the needs of a digital world. In addition, the House and Senate Commerce Committees will conduct vigorous oversight of regulatory agencies, particularly the FCC, which is pushing for net neutrality rules that Republicans oppose.

One area where members have found common ground is reform of the nation's patent laws. There is widespread, bipartisan agreement that too many nuisance infringement lawsuits have been filed and that patent assertion entities have built an industry out of suing major high-tech companies and small businesses over questionable patents.

Opposition to litigation reform does exist; mainly coming from the trial lawyer association, which generally opposes any measures that make it more difficult to file lawsuits, as well as from universities, biotech companies, and pharmaceutical companies that claim it makes it more difficult for them to enforce and license their patent rights.

However, Sen. Chuck Grassley (R-IA), the incoming chair of the Senate Judiciary Committee (which has jurisdiction over patent law), likely will not be swayed by the trial lawyers and is more likely to move legislation that will rein in frivolous lawsuits.

There also is hope that perhaps a Republican congress will act on the matter of corporate tax reform in order to drive job creation and economic growth.

Moving Forward

In the short term, it would appear Congress now has several must-pass initiatives on its plate. First, Federal government appropriations expire on December 11, 2014, so a funding bill or another continuing resolution will need to be enacted by that date.

Advancing a National Defense Authorization Act, as well as dealing with the conflict with ISIL and the challenges of Ebola will remain priorities for Congress to address.

Will this be like the productive lame duck session after the last midterm election or will there be an increased sense of urgency to act. Congress can answer this call by focusing more on the smaller, bipartisan-supported initiatives to achieve quick legislative victories, rather than getting mired in attempts to pass broad reform or controversial measures that are certain to invoke acrimony; a recipe for more posturing and ultimately, inaction.

About the Author

Bob Dix is Juniper's Vice President for Global Government Affairs and Public Policy. He was Chair of the Partnership for Critical Infrastructure Security from 2011–2014 and chaired the Information Technology Sector Coordinating Council from 2008–2009. He has been an active industry leader in efforts to improve cybersecurity and critical infrastructure protection for more than 10 years. He served as Staff Director for the House Subcommittee on Technology & Information Policy during the 108th Congress.

Modern Threats Signal Urgency for Security Strategies Overhaul

Simon Crosby, CTO of Bromium

Throughout the modern cyber era, organizations have deployed anti-virus (AV) products like bouncers at the door of a club. The bouncers would comb a waiting line of outside patrons and, if they spotted any troublemakers, they turned them away. No entry allowed.

And, for the longest time, the AV 'bouncer' system worked. Vendors came up with solutions which blocked from a network previously identified malicious code, accumulating a signature-based blacklist of "troublemakers." When new versions of malware emerged, vendors would update their AV products and proceed to continue protecting their customers.

Today, this system no longer adequately safeguards organizations, signaling urgency for a cyber security best practices overhaul. Traditional AV tactics are "dead," according to no less of an authority than Symantec – a leading player in the AV market. In fact, such techniques detect only 45 percent of all attacks, according to Brian Dye, Symantec's senior vice president for information security. The threat landscape is increasingly virulent and rapidly changing, with hundreds of millions of new malware variants created every year, according to a recent report from Forrester Research. AV tools are too reactive to keep up. By the time they find and blacklist a new attack, a wealth of others enter the equation.

For "what's the worst that can happen?" examples, we need look no further than companies such as Target, from which cyber criminals stole 40 million customer credit card numbers and 70 million addresses, phone numbers and additional items of information late last year. Then, this past May, eBay announced that a database was compromised containing encrypted passwords and other data, prompting a warning to its 128 million active users to change their passwords.

Such incidents can inflict crippling damage to the bottom line. The average cost of a breach in 2014 is totaling $3.5 million, which is 15 percent more than the average monetary burden in 2013**,** according to research from the Ponemon Institute. Then, there's the immeasurable, destructive impact on brand reputation and customer trust.

Recently, Bromium surveyed 300 information security practitioners, and 85 percent indicated that AV solutions are unable to protect against advanced targeted attacks. Not when endless forms of sophisticated malware are designed and tested to circumvent current security solutions, such as those driven by signature-based detection and behavioral analysis.

Sure, our industry can discuss in perpetuity the need for new methods and technologies. But we have to do more. We must push for a fundamental change in the very foundation of information security.

We should dispense with the 'bouncer' concept in vainly attempting to identify and block every form of cyber attack out there. Why fail in trying to defend the indefensible, when you can focus on minimalizing the extent of the damage instead? After all, it's mathematically impossible to track every single adversarial tactic out there; the bad guys will always think of new ways to hit you. Once you figure out what they're doing and invest in solutions to stop it, they'll come up with new ways to hit you again.

That's where the endpoint enters the discussion. Nearly two-thirds of the information security professionals we surveyed say they're interested in endpoint solutions. Why? Because a staggering amount of high false positives are overwhelming IT departments. And even if solutions can detect a real attack, the department *still* has to remediate at the endpoint. With a traditional AV approach, every endpoint file has to be checked against the hundreds of millions of malware variants out there. That's impossible for most, if not all, organizations.

One option, as addressed in the Forrester report, is what is described as "endpoint execution isolation" technology. This involves isolating infected apps "with logical separation between the executable and the rest of the operating environment," according to the report.

With the separation in place, the malicious code is contained within the compromised app, so it can't interact with the rest of the enterprise. Through this "micro-virtualization" of vulnerable client apps and web-apps delivered to end users, malware can't take advantage of an endpoint exploit to probe the network. Each site/app is independently isolated, with zero access to other enterprise systems, devices and apps.

Clearly, the information security transformation from an AV culture to an endpoint one will take time. Although the trustworthiness of the endpoint (or lack thereof) represents over 70 percent of enterprise breaches, it's a progression which needs to start happening now. Otherwise, the entire company is inviting risks – risks that can unleash costly fallout for months, or years. To avoid such a scenario, organizations will have to invest less into 'bouncers' and think more about protecting all of the 'club patrons' (endpoints) inside.

About the Author

Simon Crosby is Co–founder and CTO at Bromium. He was founder and CTO of XenSource prior to the acquisition of XenSource by Citrix, and then served as CTO of the Virtualization & Management Division at Citrix. Previously, Simon was a Principal Engineer at Intel where he led strategic research in distributed autonomic computing, platform security and trust. He was also the Founder of CPlane Inc., a network optimization software vendor. Prior to CPlane, Simon was a tenured faculty member at the University of Cambridge, UK, where he led research on network performance and control, and multimedia operating systems. In 2007, Simon was awarded a coveted spot as one of InfoWorld's Top 25 CTOs.

Are Your Files Protected From The Cloud?

GoAnywhere™ is a **managed file transfer solution** that tightens data security, improves workflow efficiency, 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. Features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption.

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™ → a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

SAVES US A LOT OF TIME AND HEADACHE

"It's helpful every single day as the lifeline for communications with our customers."

Matt Booher
President
WIS:DOM Information Systems

Threats are Doing Their Knock, Knock… Are We Cyber Safe for Real?

Milica Djekic, an Online Marketing Coordinator at Dejan SEO and the Editor-in-Chief at Australian Science Magazine

These days we are witnessing the time when many developed countries are issuing their warnings to possible cyber threats. It's natural that public is getting concerned because of all of that. But, what is the situation for real? Is there any reason for fear? As usual, security is supposed to be at least one step ahead of the threat, so the situation appears under control at this stage. The fact is security services must invest a lot of effort in order to maintain things acceptable, but, as you know, that's their purpose. In this brief talk, we plan to overview the current situation and to explain why we should trust our security structures.

Where Are We Today?

In a recent world, there are many threats to the western societies. Many terrorists, government and non-government hacker's organizations intend to do harm to develop country's critical infrastructure (CI). Things such as government administration's data breaches, spying on authorities and hacking a CI are getting very frequent nowadays. Security is facing up serious challenges today and this field needs very smart people to deal with all of these on regular basis.

What concerns authorities these days is the fact that the bad guys could be capable to organize, for instance, cyber sabotage to some strategically important location or they could obtain proven information about some government activities or, even worse, they could arrange a biological or chemical attack to some public spot using remotely-piloted devices.

All of these appear as a serious headache to modern security services, but what we need at the moment are good countermeasures to these events.

The question here would be if a modern security is able to protect us from all of these threats. From this perspective, it appears defense guys need to have a good learning curve and a capacity to adapt to changes such as new sorts of threats. Malicious actors and their techniques are getting highly sophisticated and their activities are getting very-well organized, so security has to be capable to cope with all of those. For that reason, defense structures need quick learners and extremely intelligent persons in order to prevent us from crime and terrorism.

Luckily, security people are certainly like that. They passed a very competitive selection; they are trained, motivated and highly skilled individuals who can meet all of these challenges and resolve the hardest issues. So, we should trust them, right?

SOCs as the Best Protection for Your CI

As our world was advancing in technological terms, safety and security requirements were getting higher and more complex. Today's period is known as a cyber age because many

industrial, technological and communications systems got computerized. CI as a vital part of the nation's infrastructure got computerized as well. In other words, these all, beginning with a simple PC at our home, over a mobile network in our neighbourhood, until the entire CI in our country, become highly sensitive and vulnerable to different types of cyber threats.

What does this mean? If we are constantly and greatly exposed to threat and if an operation of the entire country through its CI depends on computers, internet and mobile technologies, that means we need protection mechanisms in sense of people, processes and technology in order to monitor, prevent and respond to incidents within our critical systems.

The best way of protection in a modern cyber environment is through security operations centres (SOCs). SOCs represent a safety and security part of every CI complex which level of functioning can be at low, medium and high stage.

It is estimated that approximately 65% of SOCs in the US are at low level of maturity, while only 5% of them can be seen as a key force in terms of their cyber security capabilities.

It seems that we still need to work very hard in order to put our security capacities at top level of maturity. But, is that the case for real? In other words, maybe in some situations and scenarios there is no need to have a high-tech SOC, because the basic one can do a great job as well.

What we suggest here is the fact that we are still secure with our current solutions which no doubtly follow the best industrial practice and get updated when necessary.

The Importance of the Incident Response

The most serious thing that can happen in some cyber environment is an occurrence of the incident. The incident can include simple computer breach, intruder detection or inserting of some malicious piece of software into system.

Whatever happens, some steps and procedures of certain actions addressed to resolve the issue must be taken. These steps and procedures are standard part of the incident response and people who apply them are called incident responders.

Sometimes the incident response can be observed as a key factor in cyber defense. As it is known, a cyber security means a balance between prevention, monitoring and incident response.

Prevention and monitoring can be seen as passive forces in security practice, while incident response is an active principle in defense.

Although a security is a balance between passive and active actors of defense, it is intuitively clear why incident response has a crucial role in an issue management. In fact, top security systems are the ones with very-well developed incident response procedures.

Can We Remain Cyber Safe for Real?

In conclusions, a security is about a risk management, so the question on how cyber safe we are should lead us to the next one on how good we can manage our risks. The only certain thing in the future is change. How secure we will stay in the coming times depends only on how successfully we will adapt to changes.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Currently, she's the Editor-in-Chief of Australian Science Magazine, as well as an Online Marketing Coordinator for Dejan SEO. She also serves as a Reviewer and the Editor-in-Chief of the special issue "Security, Intelligence and Mobility" at the Journal of Computer Sciences and Applications. She writes for Australian and American security magazines and enjoys to share her knowledge and expertise through her lectures within her community. Milica is based in Subotica, Serbia.

Recent Regulatory Focus on Cybersecurity Fuels Financial Controls

By Joe Holman, Orangefield Columbus CEO

Recent regulatory focus on cybersecurity has placed a spotlight on the security of financial data and fueled conversations to bolster cyber controls of outside vendors that support these businesses. Concerns have emerged among managers, financial institutions, third party providers and regulators that more work is required to safeguard companies from malicious cyber-attacks, especially given recent commentary from investigators that attacks on corporate targets often occur up to 18 months before they are discovered (source).

The Securities Industry and Financial Markets Association's (SIFMA) recent call to arms for U.S. financial firms and regulators to join forces and create a system for sharing information on cyberattacks in order to mitigate future threats is a step in the right direction. However, financial organizations must understand what data is most valuable to attackers, their greatest points of vulnerability and the solutions available to solidify their operations.

Cybersecurity Challenges

In April, the Securities and Exchange Commission (SEC) issued a checklist that was intended to help firms review their controls to combat cyberattacks. In July, the U.S. Department of the Treasury's financial crime enforcement network (FinCEN) issued a notice on pending regulations around Customer Due Diligence Requirements for Financial Institutions.

And now New York State's top financial regulator Benjamin M. Lawsky has requested a dozen banks provide their policies and procedures for governing relationships with third party providers and outline their due diligence processes.

With this increased scrutiny from U.S. regulatory bodies, a sense of urgency has developed among firms, particularly within the asset management and fund management spaces, to put in place sufficient and proper controls to detect and prevent data breaches.

In a recent whitepaper from the Depository Trust & Clearing Corporation (DTCC), only 84% of respondents in financial services identified cyber risk as one of their top five concerns despite evidence from a survey by Kaspersky Lab and B2B International that indicated 93% of global financial services organizations experienced various cyber threats between April 2013 and May 2014.

Some firms, however, are failing to take precautions toward data protection. In some instances, basic and essential safeguards fall to the wayside that should not: some firms do not obtain

updated software systems, some have inadequate password conventions and firewalls, and others do not know how to safely transmit confidential information.

With the right security and software however, confidential information and the integrity of a fund's data can be protected.

Cybersecurity Best Practices and Points of Vulnerability

Fund managers should have compliance policies and procedures in place for protecting data. To this end, firms must look to identify the sensitive types of data shared with third parties that should be granted a certain level of security against hacking. Data types that are of the utmost importance to protect can include non-disclosed financials, portfolio financials, deal-making financials, confidential trading data and non-public, market making data, and investor information.

Breaches that access these data types could potentially have severe impacts on firms and the wider marketplace, depending on whether information is stolen, tampered with or manipulated in some other way. At stake for firms that use legacy non-secured systems can be financial losses, a negatively impacted corporate reputation, and even regulatory investigation and fines.

For example, the Poneman Institute found in a study of 59 firms it recently conducted for Hewlett-Packard that the annual cost of dealing with cybersecurity among financial services companies was estimated to average $20.8 million in 2014.

Overall, there are a number of measures and controls that technologists at fund managers can take to ensure they are adequately securing financial information. In relation to third party providers, it is essential for funds to have a strong due diligence process in place for vetting their vendors and any counterparties with which they do business.

For instance, it's important to understand what a third party's internal policies are for protecting and securing data, and also what a firm's contract with them requires in terms of data security.

In conducting due diligence around their third party's cyber controls, fund managers can minimize the risk of an attack on their confidential data through their third party providers and gain a greater understanding of their larger network infrastructure.

Proactive due diligence combined with ongoing workflow reviews either manually or through technology will allow firms to *anticipate* attacks and monitor patterns for signs of possible breaches. This element of defense is essential in order to prevent data breaches altogether and stem the costs of responding to hacks.

Increased regulatory focus on cyber regulations illustrates that the discussion of how firms can better protect themselves against cyber-attacks is not going away anytime soon. As the

conversation on the role of regulators in this process evolves, it is essential for firms to stay informed, alert, and be proactive.

About the Author

Joseph Holman is the CEO of Orangefield Columbus. Prior to joining Orangefield Columbus, Mr. Holman founded Columbus Avenue Consulting in 2004. He has over 25 years of experience in the financial services arena, with a particular emphasis on fund administration and business development.

Mr. Holman began his career as an accountant with Paul Scherer & Company in 1986. From 1990 to 2004 Mr. Holman worked with Rothstein, Kass & Company P.C. where he was named a Shareholder in 1998. While at RK, he played an integral role in building the fund administration and audit practice, as well as offer expert advice to clients on regulatory, operational and tax related matters.

Mr. Holman holds a BS in Business Administration from Clarion University of Pennsylvania and an MBA from Rutgers Graduate School of Management. He also attended the MS in Taxation program at Seton Hall University. Mr. Holman is a CPA and member of the AICPA. He is recognized as an industry expert and is regularly invited to speak at conferences on topics such as hedge fund accounting, valuation and best-practices.

2014 SMART CYBER DEFENSE

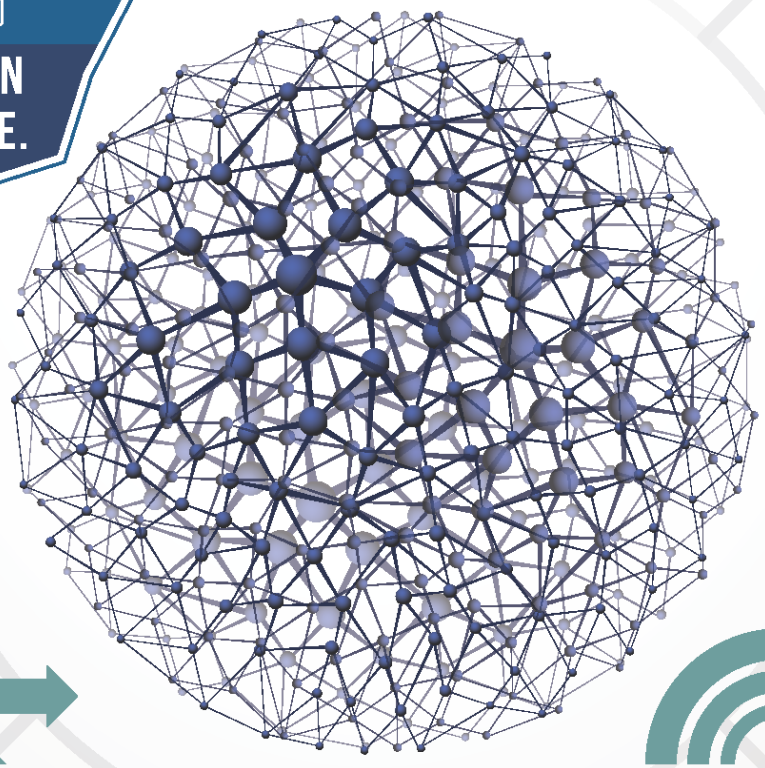
CAXTON TECHNICAL TRAINING COURSE

23 - 27 NOVEMBER 2014 | ABU DHABI, UAE

REGISTRATION IS NOW OPEN. CHOOSE FROM THE 2 COURSES OR SIGN-UP FOR THE COURSE BUNDLE AND

SAVE 10% ON TRAINING FEE.

TO REQUEST FOR INFORMATION OR TO REGISTER,
CONTACT: KRISTINE TUAZON EMAIL: KRISTINE.TUAZON@CAXTONGROUP.COM
TELEPHONE: +971 4 276 5897 EXT. 126



SMART CYBER DEFENSE COURSE 1:
SOLID DEFENSE STRATEGIES

SMART CYBER DEFENSE COURSE 2:
DISASTER RECOVERY AND CYBER INCIDENT RESPONSE

"THE MUCH-AWAITED **SMART CYBER DEFENSE TRAINING COURSE** IT PROFESSIONALS HAVE BEEN LOOKING FOR."

www.caxtongroup.com

Q&A with Tim Clark, The FactPoint Group, on Automated Malware Removal

By Todd Weller, VP, Corporate Development, Hexis Cyber Solutions

Earlier this year, one of the biggest U.S. hospital groups, Community Health Systems Inc. (CHN) publicly announced that it was a victim of a Chinese-driven cyber-attack. The attack, led by hacking group "APT 18," stole Social Security numbers and other personal data belonging to 4.5 million patients within the organization's network. This is just another instance of advanced hackers infiltrating the network of an unsuspecting organization.

These unfortunate occurrences have left many companies scratching their heads and thinking, "Is there any way to truly protect our data?" Inadequate defense technologies that attempt (but more often than not fail) to quickly remove threats are leaving end-users vulnerable to an attack. Is there a fail-safe approach to better security? Tim Clark, partner at The FactPoint Group and security industry expert believes that automated malware removal is key to any effective security strategy. Here's what he had to say:

1. **Why are companies so scared of automation?**

   Security professionals are nervous about automated malware removal because they don't really understand it. While it may just be an overall messaging problem that our industry needs to address, many equate the term "automated" to turning an entire process over to a machine – an act that leaves many feeling uneasy and with little control. For dealing with Advanced Persistent Threats (APTs), a handful of organizations focus on leveraging technologies that prevent and/or remediate the issue – instead of completely removing the malware itself. When malware is simply contained or isolated, it leaves an opportunity for sophisticated malware to re-infect the system.

2. **Why should companies embrace automated malware removal?**

   Attackers are advancing, incidents are increasing and the number of qualified security professionals can't keep pace. Companies are still dealing with the aftermath of the recession; they don't want to invest in things that don't drive revenue, i.e. security professionals. To them, security doesn't produce revenue. While that may be true, security does protect revenue. Automated malware removal helps to address the tight budget problem. It allows for the routine incident response work of initially recognizing malware to be done by a computer so that the highly skilled security pros can be working on more difficult, advanced problems – not wasting time on clerical work.

3. **How can companies make automated malware removal work for them?**

   When it comes to implementing automation, there are a few best practices that companies should consider. First, to minimize the risk of false positives, security professionals should leverage both historical information and forensic analysis of malware. Do the work. Second, these same security pros should automate certain tasks they feel comfortable with by setting

policies on what should be automatically removed, what should be detected by a machine and later flagged for human decision, and lastly what can remain on the network. Enabling that range of policy-driven responses to suspected malware is incredibly important for staying within the varying comfort level of security professionals; some may want to automate the process of killing identified APTs while others would prefer to automatically quarantine suspicious code. Allowing security professionals to automate what they want and no more is a key capability for automated malware removal software.

Interested in learning more? Download Clark's whitepaper, "The Case for Automated Malware Removal" for an in-depth overview on why automated malware removal is the key technology for fighting Advanced Persistent Threats.

About the Author

Todd Weller, VP, Corporate Development, joined Hexis Cyber Solutions in March 2014. His responsibilities include analyst relations, competitive and market intelligence, corporate visibility, M&A, and strategic partnership development. Todd draws on his 17+ years of experience as an equity research analyst where he covered the security industry for much of that time. In his equity research career Todd provided research coverage of over 60 companies across several technology sectors, including security, infrastructure software, data center/cloud hosting, and healthcare IT.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

What is Data Security in the Cloud?

The past two decades have seen rapid progress in technology. While the internet revolution has connected businesses around the world, cloud computing technologies have optimized resources. The Internet of Things (IoT) brings a versatile range of devices into the network. Gone are the days when communication was only possible between computers. The IoT revolution makes it possible to transmit data across a range of devices. Unfortunately, the advances in technology are accompanied by data security threats.

According to the Cisco Visual Networking Index, global IP network traffic is more than 1 zettabyte per year, or 91.3 exabytes per month. This value is expected to reach 1.6 zettabytes per year by 2018, equivalent to 45 million DVDs per hour. With such huge volumes of data traveling on the network, hackers have the incentive to develop scripts to capture data.

The Identity Theft Resource Center (ITRC) reports that 666 data breach cases were identified between January 1, 2014 and November 12, 2014, the medical and health-care segments being worst affected. Whether big or small, data breaches can severely affect the revenues of a company. Until recently, 80% of data loss was caused by company insiders. However, this situation is changing. With the ever-evolving internet trends, data security threats are increasing exponentially. Data security must be addressed in many dimensions.

What is Data Security Within Organizations?

Within an organization, the entire network must be securely deployed, so that unauthorized users cannot gain access. Moreover, it is important to hire reliable personnel to manage databases and system administration.

When managing data, it is advisable to streamline procedures, so that different privileges are assigned to different users based on their job roles. Data management has to be augmented with efficient technology that enforces system policies properly for secure access to data, and its storage, retrieval or manipulation.

What is Data Security Outside Organizations?

The internet revolution has created integrated business systems whereby employees, clients and customers can access corporate information from anywhere, at any time. While this flexibility creates more opportunities, data security is at risk. Data traveling between networks may be subjected to tampering, eavesdropping, identity theft, and unauthorized access. Network encryption and access controls that are augmented with a higher level of authentication are required to securely transmit data.

What is Data Security in the Private and Public Cloud?

Today, everything resides in the cloud. In 2012, Gartner predicted the transition of offline PC systems to the cloud by 2014. The prediction was accurate. The majority of enterprises use at least one model of cloud computing technologies to carry out business procedures. However, increased agility and economic benefits come at a price. With the cloud and virtualization technologies, businesses have logical control over the data, but the actual data reside on servers managed by third party providers. When multi-tenants share the infrastructure, data integrity is compromised. Moreover, data compliance issues may arise when data reside away from company premises. Customer privacy needs to be maintained. Data segregation techniques matter. Without clear visibility into operational intelligence, companies have to rely on third parties' security solutions. In case of data disaster, businesses should be able to retrieve data and services. If a cloud provider is acquired, data and services should still be securely maintained.

The traditional network-centric security solutions, such as intrusion detection systems and firewalls, cannot protect your data from hacking by privileged users and advanced persistent threats (APTs). There are other methods, such as security information and event management (SIEM) and database audit and protection (DAP), for event correlation. With stringent data regulations in place and increased data breaches, businesses have to move from network-centric solutions to data-centric solutions by integrating data security intelligence and data firewalls to create a veritable firewall around the data. Strong access controls, key management and encryption that are augmented with security intelligence are required, because once you move everything into the cloud, you only have a web browser as an interface.

What are Data Security Law and Policy?

The Data Protection Act 1998 is a British law that regulates the processing of data on identifiable living people. It controls how organizations, businesses and the government use the personal information of users. While businesses have to cope with rapidly exploding big data, they have to work in compliance with data protection laws, which are more stringent when sensitive information such as ethnic background, religious beliefs and criminal records are involved. As opposed to Britain and the European Union, the United States does not yet have a consolidated data protection law, instead adopting privacy legislation on an *ad hoc* basis. The Video Privacy Protection Act of 1988 and the Massachusetts Data Privacy Regulations of 2010 are a couple of examples.

When it comes to the cloud, there are no borders. A company located in one country might use CRM solutions offered by another company that is based in a different country. In such cases, it is not easy to know where the data are stored, how they are processed and what data protection laws govern them. Businesses that are moving into the cloud should enquire about data management by the cloud provider.

What is Data Security in a Private Cloud Solution?

While resource allocation and data security are the prime aspects of concern in the public cloud, deployment of a private cloud is a totally different ball game. In a private cloud, data are stored within your company's perimeter, behind a dedicated firewall, and are securely accessed through encrypted connections. Data are always stored on your server, and remote users only get projections of data on their devices. Moreover, a private cloud provides greater control over redundancy, because you address your redundancy requirements when designing your data center environment. With the hardware being on-site, businesses have more control over data monitoring and management. Data compliance is effectively met. While businesses can enjoy the scalability, agility and mobility offered by the cloud, security and business continuity are maintained at the highest level. Applications hosted in the private cloud require less administrative overhead and reduced customer support, while ensuring that only the latest versions of applications are used. However, higher costs, capacity ceiling, and on-site maintenance are a few aspects that should be considered. The key is to choose the right tool that delivers a secure cloud environment.

2X Remote Application Server (2X RAS) is a leading software solution that allows companies to manage and deliver virtual applications and desktops from a private cloud. The flexibility of the product allows companies to leverage different hypervisors, such as Hyper-V, VMware and Citrix. With 2X RAS, organizations can guarantee secure access to corporate applications and data from any device. The SSL encryption secures transmission of data between the device and the server farm. The wide range of compatible devices makes 2X RAS one of the most effective solutions available. 2X RDP Clients and Apps for 2X RAS are available for Windows, Mac, Linux, Android, iOS, Windows Phone and HTML5. Click here to read more about 2X RAS.

References

What is Data Security? | The Zettabyte Era — Trends and Analysis | cisco.com
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html

What is Data Security? | Data Breach Reports | Identity Theft Resource Center
http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

What is Data Security? | Gartner Says the Personal Cloud Will Replace the Personal Computer as the Center of Users' Digital Lives by 2014 | gartner.com
http://www.gartner.com/newsroom/id/1947315

What is Data Security? | Data Protection Directive | wikipedia.org
http://en.wikipedia.org/wiki/Data_Protection_Directive

What is Data Security? | Data Security | techopedia.com

http://www.techopedia.com/definition/26464/data-security

What is Data Security? | What is Data Security? | spamlaws.com
http://www.spamlaws.com/data-security.html

What is Data Security? | Data security | bbc.co.uk
http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/6datasecurityrev1.shtml

What is Data Security? | Data security definition | qas.co.uk
http://www.qas.co.uk/knowledge-centre/support/glossary/data-security.htm

What is Data Security? | Top 10 ways to secure your stored data | computerworld.com
http://www.computerworld.com/article/2546352/data-center/top-10-ways-to-secure-:your-stored-data.html

What is Data Security? | Protecting Data | ist.mit.edu
https://ist.mit.edu/security/protecting_data

What is Data Security? | What Are the Risks to Data? | ist.mit.edu
https://ist.mit.edu/security/data_risks

What is Data Security? | Data security | data-archive.ac.uk
http://www.data-archive.ac.uk/create-manage/storage/security

About the Author

Giorgio Bonuccelli is the Marketing and Communication Director for 2X Software. Giorgio has extensive experience in cloud computing and virtualization, with a background of many years in multinational corporations (Dell, EMC and McAfee). In his career he has filled different roles, from sales to training and marketing. This wide-ranging experience and flexibility helps him simplify concepts and write content that is easy to read and understand even by newcomers to the subject. As a blogger and technical writer he has published more than 1000 papers.

ForgeRock Delivers Solution to Help Government Agencies Accelerate Secure Rollout of Digital Services For Citizens

With data breaches impacting millions of Americans, President Obama signed an Executive Order on October 17, 2014, that emphasizes securing online transactions. The National Strategy for Trusted Identities in Cyberspace (NSTIC) office is overseeing progress towards meeting this mandate, which will likely require federal agencies to connect with the United States Postal Service's (USPS) Federal Cloud Credential eXchange (FCCX). The FCCX is a federation hub that allows citizens to securely access government agency services with existing commercially issued, verified digital identities. The FCCX acts as a middleman, streamlining citizen access to online services with a secure, privacy-enhancing, easy-to-use-solution while also reducing costs for government agencies.

The Executive Order calls for plans to be presented to the President within 90 days and for agencies to comply within 18 months. In anticipation of these plans, ForgeRock Inc. recently announced FederalConnect, a new downloadable software solution that allows federal agencies to accelerate their rollout of digital citizen services. ForgeRock, a leading open-platform provider of identity and access management solutions, already has an impressive track record in delivering eGovernment authentication, having provided the platform for digital services targeting citizens for the governments of Norway and Belgium. The company has also begun working with the U.S. Department of Homeland Security.

Widespread adoption of eGovernment practices is likely to ease citizen access to services and deliver substantial efficiency gains to government agencies. The IRS, for example, spent more than $1 billion communicating with taxpayers on paper and by telephone in 2012 but could slash these costs if more citizens communicated with it online. Compared to the costs of building and maintaining its own identify authentication solution, the IRS could save $63 million to $298 million during a 10-year period by using FCCX to authenticate citizens. The agency could save between $40 million and $110 million in adoption costs alone.[1]

Effective eGovernment Needs a Hub

U.S. government agencies and departments have traditionally had their own applications and authorization processes, but multiple sign-ons, digital IDs, and passwords are difficult for citizens to handle and pose a security risk because identifying information is passed around multiple networks and systems. With fresh reports of security breaches coming out almost every day, citizens have become wary of providing identity information online. This acts as a drag on their adoption of online services—and prevents the government from realizing the full potential

[1] http://www.slideshare.net/CloudIDSummit/03-grant-fccx-and-idesg-and-industry-perspectives

of eGovernment efficiency and cost savings seen in other countries around the world. For example, in Norway, nearly 100 percent of its citizens and 500,000 businesses now access more than 300 government services online, resulting in significant cost savings—and extraordinary improvements in efficiency.

How FCCX Works

FCCX uses federation for single-sign, on so it doesn't spread users' credentials around multiple systems. Agencies allow user access based on a secure handshake with FCCX, without requiring it to pass on personal credential information. This "circle of trust" leverages security assertion markup language (SAML), the XML-based, open-standard data format for exchanging authentication and authorization data. The latest version of SAML, V 2.0, creates a standardized, cross-domain, web-based, single-sign-on framework. The government chose SAML because relying on open-source standards is a proven way to reduce spending, increase efficiency, and provide extra security validation through transparency.

Private businesses—companies such as Google and Facebook—will be able to offer users access to FCCX through their existing credentials. First, though, they will need to be certified through the FCCX-approved identity and authentication provider. The Kantara Initiative—which helped to design SAML V 2.0—is the Trust Framework Provider for the U.S. Federal Identity Credential Access Management (FICAM) team and will provide policy and technology interoperability verification for businesses that seek to connect to FCCX.

"We've always known that open standards could add considerable value in enabling effective eGovernment and are pleased to see the direction that NSTIC and FCCX are taking on this," said Allan Foster, president at Kantara Initiative. "We look forward to seeing widespread adoption of open-source-based products such as ForgeRock FederalConnect to help federal agencies quickly connect to FCCX."

How agencies can connect to FCCX

For federal agencies, it will be a relief to get out of having to manage citizen identities—but first they have to come up with a plan for connecting to FCCX and execute on that plan within 18 months. Most agencies are likely to evaluate commercial software based on SAML, because they want vendors to add value to SAML with the same support, rigorous product-development processes, and testing that agencies expect from proprietary software. And agencies will be making their evaluations with their eyes on the clock: the 18-month timeline means they need ease of implementation and a proven track record. Any product that promises pre-packaged integration with FCCX is likely to jump to the top of the list for evaluation.

SAML-based FederalConnect fully meets agencies' requirements. A lightweight packaged commercial open-source solution, it allows agencies to avoid complex integration efforts: they

don't need to deploy infrastructure on their servers and can change a few lines of code in their applications to connect to the FCCX hub in days or weeks instead of months or years.

Looking forward

The need for FCCX has been building for years. It's a necessary first step, and once it's in place, chances are that there will be calls for additional security features, such as multi-factor authentication or contextual authentication and the use of real-time data and analytics to evaluate user risk. This future could arrive soon: the Department of Homeland Security is already rolling out the use of digital identities and using contextual authentication from ForgeRock in managing first-responder access to government buildings.

Unfortunately, there's no end in sight for the ongoing security race between hackers and government agencies. But at last, with this mandate, there's a secure way to start providing U.S. citizens the full benefits of eGovernment, from easier access to services to more efficient use of their taxpayer dollars.

Wondering why USPS was chosen for this project? Here's what the agency's website says.

USPS runs one of the world's largest computer networks, including one of the largest email systems, handling more than four billion communications annually, with more than 13 million external email messages scanned for viruses every month. This, combined with the unique law enforcement resources of its Postal Inspection Service, makes the Postal Service ideally suited to support the FCCX pilot project and the development of a secure credential exchange for the federal government.

About the Author

Daniel Raskin, Vice President of Strategy, ForgeRock

Daniel has more than 15 years of experience building brands and driving product leadership. Prior to joining ForgeRock, he served as Chief Identity Strategist at Sun Microsystems. Daniel has also held leadership positions at McGraw-Hill, NComputing, Barnes & Noble and Agari. He holds a master's degree in international management from Thunderbird School of Global Management and a master's degree in publishing from Pace University.

CI Energy Group's Inaugural Summit on

Cyber Security *for* Energy

January 21 – 22, 2015 » TELUS Convention Centre » Calgary, AB

The intelligence and tools you need to protect critical assets from cyber attacks

Global cyber-attacks on critical infrastructure continue to increase in frequency and Canada's energy sector is by no means exempt. Hacktivism, state sponsored attacks, cyber terrorism and industrial espionage are but a few of the emerging threats facing the oil, gas and utility sectors. Antiquated strategies, such as anti-viruses and firewalls are no match for the sophisticated hackers of today. Senior executives and their respective organizations must take a proactive and technologically-advanced approach towards cyber security if they hope to safeguard critical assets and avoid damaging and costly liability claims.

CI Energy Group's Inaugural Summit on Cyber Security for Energy was designed in tandem with the country's leading experts and promises to deliver the up-to-the minute information and critical strategies your organization needs to make sound security planning decisions.

Hear from Leading International Experts including:

- Shell Canada
- North American Electric Reliability Corporation (NERC)
- Enbridge Inc.
- Nexen Energy ULC
- ENMAX Power Corporation
- TransCanada

Hear Vital Information to Inform your Security Planning:

- Understand the latest threats targeting the Canadian energy sector
- Conduct thorough vulnerability assessments for oil, gas & utilities
- Learn innovative and effective approaches for planning, preparing and responding to cyber incidents
- Protect SCADA systems from emerging cyber threats
- Evaluate the Board of Directors' oversight into cyber security
- Assess Canada's cyber security regulatory framework and understand how it can be improved

Benefit from hands-on workshops:

A **A Step-by-Step Guide to Conducting Vulnerability Assessments**

B **A Primer on Planning, Preparing and Responding to Cyber Attacks**

PRESENTED BY: CI Energy Group

SPONSORED BY: CGI, Check Point Software Technologies Ltd., iON Secured Networks, Fortinet, intel Security, Symantec, TELUS, THALES

MARKETING PARTNER: CDM

Priority Service Code: 270DX02

REGISTER NOW » 1-877-927-7936 » **www.CanadianInstitute.com/CyberforEnergy**

Web Server Security – Mind it before you hacked

Web servers are one of the most targeted platforms for hackers because of the sensitive data that they host. The security of the web server is as important as the security of a website or web application. In current time, web server security is an intimidating task for server experts. If you have a security for a website or web application, but not having security for web servers, then your business is at risk. Many hackers are using advanced techniques to steal user data without their awareness. We use antivirus software or firewalls for protection of our PC, but we usually forget to secure web server that can cause damage to online data. Data security has become crucial for any web server and securing a web server is a relief against data theft and other online frauds. This article focuses on some significant measures on web server security.

Security for Web Application: The web server is always sensitive to attacks due to an open access platform. Any vulnerable script on the server can cause an attack on the server; therefore, it is necessary to make them secured. A mere firewall cannot protect online attacks so a proper network security is necessary for the web server. Even turn off all unused ports on the server will reduce the risk of online attacks. Always set up your server offline, and upload patches through an external device. This ensures that your web server is more secure. Before placing your server online, make sure that it has vigorous protection.

Monitor: Monitor your web server, database server or any imperative systems for any potential warnings and attacks. You can use the system logs for monitoring and scan tools for finding vulnerabilities. Many tools will send you a text message for any occurred problem. With monitoring, you can notice threats and potential attacks before they create troubles. Any strange log entry should be observed to prevent such attacks.

Get help out: Get the support of forums, blog, video tutorials, for server security solutions. It is advisable to get premium support services, but if you cannot; then go for the free service. If you can pay then it will act as a better security consultant. Web hosting provider also provides a variety of a managed server alternatives.

Remove needless Service: In case of default installation, many needless services like remote registry service, print server service, RAS, etc. will be installed on your server, which left more port insecure to be abused by malicious hackers. To prevent malicious attacks, you must close all needless services so it may not start automatically after rebooting the server, and this will enhance the performance of the server.

Remote Access: Remote connections should maintain securely with encrypted protocol. Remote access should include specific IPs and accounts. It is advisable that never use public computers or networks for remote access of the company server like public internet cafe or public wireless network. You could be a victim if you are using public networks, hackers can easily hack your server by sending malware or threat in your system.

Testing & Development: Development and testing of web application must have separate environment. Web application in their earliest stage of development could suffer from numerous vulnerabilities and it is unable to handle exceptions. Such applications are on target of hackers and could easily be revealed and exploited. To make easy development process of web application, web developers should develop internal applications for exclusive right to access web application. It is sensible for developers, not to test web applications on production server. However, testing and development process must be done on servers inaccessible from the internet.

Web Application Content: Website scripts and application files should always be on a separate drive rather than an operating system, system files, and log files. Hackers can easily gain access to the web root directory and exploit vulnerabilities to gain access of operating system, log files, or system file those results in total control of the web server in hacker's hand.

Exclusive right: Network service software runs some specific files and if the web server engine is exposed via network service, then hacker can abuse server account. Therefore, there should be less exclusive rights to run network services like web server software. A user who accesses a website, web application files, data backup, and database should have minimal rights. Thus, the web server will remain secure.

User accounts: Default user accounts made throughout an installation of operating system should be canceled. Some software at the time of installation require a user account which should be closely monitored and if require it must be restricted for the privilege. Administrator account should not be used for other system installation like Linux/Unix system. Administrator who access web server must have different passwords with exclusive right. The administrator should never exchange or share their passwords with each other.

Updates: Many software companies release updates for software to prevent potentially malicious attacks. Thereby they want to make their software better for the future usage. It is important to know about upcoming tools (scanning, penetration testing, etc.) and threats with the help of security magazines, newsletters, articles so you can take further steps to secure your web server in a better way.

Multitasking: Many companies run different functions on a single server that could become serious for web server security. If a hacker compromised your server, all the functions would be exploited. Therefore, each function should have a dedicated web server to make your task simple and prevent malicious attacks.

Web server security is a difficult task, but not an impossible task. If you take care of your web server by following the above steps, you can stop malicious attacks. Unrelated web server software and operating system running on your web server or an outdated configuration is typically deemed insecure. It is desirable to have a enhance security of your web server.

About the Author

Keeping pace with the ever-changing technology and marketing paradigm, Gunjan Tripathi has been rendering service as a digital marketing expert at CheapSSLShop.com. As he is involved in info security field, Gunjan likes to contribute in cyber security awareness and writes on several topics in information security.

WHAT TO EXPECT

EXHIBITION SPACE

27,000 SQM

EXPECTED NUMBER OF EXHIBITING COMPANIES

250

EXPECTED NUMBER OF TRADE VISITORS

8,000

450
KEY DECISION-MAKERS FROM INTERPOL'S

190
MEMBER COUNTRIES

Contact us TODAY at +65 6389 6614 or sales@interpol-world.com

Event Owner: INTERPOL

Supported By: Ministry of Home Affairs; Singapore Exhibition & Convention Bureau

Supporting Knowledge Partner: Frost & Sullivan

Held In: YourSingapore

Managed By: MP international

Is it ethical to sell zero day exploits?

Zero day flaws are the application vulnerabilities that nobody knows about until it's too late. They're the things like Heartbleed, or Shellshock, or most recently POODLE that allow hackers and attackers to execute malicious code on machines that aren't theirs. They're also the things like Sandworm and Operation Snowman: previously unknown entry points into a PC through end user software that allow malware writers to infect their victims in new and often unprotected ways.

Zero days are dangerous because once they are announced users literally have **"zero days" to apply a patch**. Once a zero day is made public, you can already assume it's being exploited by cybercriminals in the wild. For this reason, the biggest concern in the world of zero day research is never an issue of when – as bugs will always be discovered. Much more pertinent is the uneasy question of how.

How Zero Days are Disclosed

Zero day research is a very big deal, and it **involves a lot of money**.

On one end of the spectrum, you have internal researchers, employed by software companies, who actively look for security flaws in the company's product, so that they can stay ahead of attackers. If zero days are ever found, the software receives "just another round of updates" and the problem is more or less silently fixed, without a scary security announcement to users.

This is, for example, what happens with your Windows-based PC on the second "Patch" Tuesday of every month. Patches like these are by no means perfect, as there is always a small time window between release and automated update that attackers can exploit, but 'good guy' zero days more or less make the best of what's already a bad situation.

On the other end of the spectrum, things get much worse. Here, you have financially motivated hackers who uncover new vulnerabilities all on their own.

They have no ties to the company or the users their discovery will affect, and they simply want to make as much money as they can, regardless of others (or the law). In this 'bad guy' scenario, a profitable course of action is keeping one's mouth shut and silently adopting the zero day in a new malware distribution campaign. In this way, a bot master can infect thousands of new victims in a matter of days. His in-the-wild zero day will of course eventually be discovered by one systems administrator or another, and eventually announced, and eventually patched – but all of that takes time.

Go between these two endpoints, and **things start to get interesting**. Sometimes, the good guys aren't official employees – sometimes they're independent researchers applying for bug bounties, which at big companies like Facebook and Microsoft can be as large as $150,000.

Sometimes these researchers get their bounties, along with 15 minutes of fame, and other times they do not. When this latter scenario occurs, things begin to turn a bit greyer, as jilted researchers sometimes opt to **disclose to the public** without the affected company's consent.

In situations like this, the company is usually spurred to action – but whether users are safer than they would have been if no one ever knew is a hot topic of debate. You can't know what you don't know, and with zero days, this means that there is always the chance that someone malicious has discovered it too. For the surveillance wary, this 'malicious someone' even extends to the government; in fact, in recent months, some have even suggested that the NSA knew about Heartbleed.

Zero days, get your zero days!

So, who else finds zero days? Well, a better question might be: what happens when zero days become a commodity? What happens when a few entrepreneurial actors come along and recognize that the spectrum outlined above represents much more than just a collection of ways in which software flaws are discovered and disclosed? When they realize, with glee, that this spectrum is a real-life environment, *overflowing with unmet economic demand*?

Enter the world of **for-profit zero day research**. Here, vulnerabilities are bought and sold to the highest paying bidder.

Here, vulnerabilities aren't just casually researched by security enthusiasts hoping to make the world of software a better place, and maybe make a few bucks while they're at it. Here, zero day flaws are aggressively sought after – and when they're found the danger of public disclosure is used as a very effective sales mechanism.

It **works like this**:

Someone comes to your place of business and tells you they have discovered a secret way to exploit your product that will allow whoever uses it to leech money and personal information off of you and your customers.

They tell you that you can have access to this secret information, but only at a price. You freak out, but then you think: should I take this person seriously? Then you consider slamming the door on them. Then you realize: if what they're saying is true, what's stopping them from selling this supposedly secret knowledge to someone else?

From a **legal standpoint**, nothing is stopping them. For-profit zero day research, and even brokering, is completely legal. This is because the *knowledge* of a zero day is not the same thing as the *exploitation* of a zero day. Knowing a flaw exists is not illegal to know, and for companies that have such flaws this knowledge can help prevent security disasters. The problem, though, is that this knowledge isn't always sold to the companies it affects. It's sold to whoever is willing to pay, based on the seller's discretion.

Sometimes, it's sold to competitors. Other times, it's sold to governments. Pricing can range from 5 to 7 figures, and many of the larger customers actually pay for catalog-styled subscriptions that give them access to 100-or so industry vulnerabilities, per year.

Smaller software companies, on the other hand, usually cannot afford to play this zero day game. This often means that independent researchers don't bother to find flaws in smaller company's products, even if the products are good and lots of people use them. It can also mean that if zero days affecting smaller companies are found, for-profit researchers stand to earn much more by selling the knowledge to a larger (walleted) competitor and never telling the affected company or its users.

The firms that find and sell these vulnerabilities can be found through a simple Google search. There are many, and anyone who runs this search will also find that scattered throughout the results there are also more than a few articles on ethics.

Zero day **knowledge** may be fundamentally different from zero day **exploitation** – but the question of whether people should sell the former to prevent the latter remains unresolved. In a free market vulnerability economy, the only thing stopping a research firm or broker from selling a zero day to a cybercriminal or repressive government is that research firm or broker's moral compass. Many feel that this barrier is much too subjective and much too easily swayed by the amount of money that is involved. Many also worry at the fact that most zero day salesmen have sworn to keep their client lists absolutely secret.

For users affected by security bugs in the products they buy to manage their work and their lives, the question that needs to be answered is whether for-profit zero day research has a net positive or net negative effect.

Fundamentally: Is software safer in a world where zero day research is privatized? Or is vulnerability salesmanship simply Malware Lite?

As always, we'd love to hear your thoughts.

Have a great (zero-free) day!

About the Author

Steve Nowicki is a freelance writer from Illinois. He has an interest in how people interact with technology and how these interactions continue to transform society. You can find more of his work on information security at the Emsisoft Blog.

Unconventional Fraud

Luis Corrons, Technical Director of PandaLabs

The current malware environment is sophisticated and widespread. Long gone are the days when traditional attacks occurred by just clicking on a malicious link. Internet fraud and cybercriminal activity have become so much more insidious and undetected, but has evolved around the same intent of stealing money and personal information.

One major fraud campaign has been evolving over the course of decades and really demonstrates how far cybercriminal activity has progressed.

Operation Oil Tanker

Typically when we think of the oil industry, the Middle East immediately comes to mind, but there are many countries that are major oil producers. There is a region in Nigeria called Bonny, well-known for its production of highly-valued Bonny Light Oil. It has very low sulfur content, which translates into low corrosion in refineries, causing for high demand worldwide.

Whenever there is a high demand for a product and a lot of money in an industry, there is a high probability for fraud. There is an old scam in the oil industry of Nigeria that typically involves promising the victim a significant share of oil, and requiring a small up-front payment to obtain. The fraudster offers false certificates for proof of product and if a victim makes the payment, the fraudster disappears. The article of the Nigerian Criminal Code that refers to this type of fraud is number 419. Although this con had been used with traditional mail in the oil industry, it has been given new life with advancements of the Internet.

First Sighting

In January 2014, a new threat was detected in the network of a leading shipping company in the UK. Malware experts started studying the threat, and saw it was prepared to steal emails and browsers' saved credentials, and planned to send them to an external FTP site. The experts gained access to that FTP and looked for stolen credentials in case their computers were not properly protected. They discovered that the FTP did house approximately 80,000 text files with stolen credentials, 90MB of user names and passwords. Due to the large amount of information, it wasn't immediately identified as a targeted attack, but the experts determined that some of the data had been stolen more than six months prior. Upon further investigation, experts found that this fraudulent activity originated from the oil industry, linking it back to this history of oil fraud and confirming it was a targeted attack.

The Process

As mentioned earlier, the scammers need certificates in order to scam the oil buyer. They can make up those documents, but by doing so, risk to be discovered. However, if they get access to real companies and create certificates with actual information, the buyer trusts the seller to complete the business transaction.

The initial attack comes in an email with an attachment. The file uses a PDF icon and the file name is “Document.exe.” Once opened, a black PDF document appears, but otherwise no other visible actions are noticeable. The smart thing about this attack is that it can be said it does not use any malware to perform its malicious actions.

The original file is an installer, it contains a number of files and the only thing it is doing in the computer is creating a folder and unzipping files into it. Then it executes one of the files and exits. This starts the “infection” process, where it will run a number of different script files, one after the other, and each one performing just a few tasks in order to avoid raising any alarm, going unnoticed. These tasks go from creating registry entries to ensuring it will run every time the computer starts, stealing all browser and email saved credentials (using legit freeware software tools that let users recover saved credentials) and uploading them to an FTP.

And that is it, an easy way to steal credentials without using any “real” malware. It goes through the credentials process every hour to capture any new saved username and password in the system.

Who is Behind this Attack?

One of the weaknesses of using this kind of approach is the way the stolen credentials are sent. Since it used the FTP command from one of the bat files and the same command included the user name and password to access it, that is how the malware experts were ultimately able to access it and download all the files.

The criminals behind this attack were using a free FTP service, and would access the control panel with their credentials, where you could see all the information that the attackers had filed to get the free FTP account, such as first and last name, country, city, zip code and email address.

Of course this information was false. But where it became interesting was that the city listed was Ikeja, a suburb of Lagos, the capital of Nigeria. Ikeja is known as the “Computer Village” for its large computer market. Even though this didn’t mean the criminals were from Ikeja, this at least inferred they were either from Nigeria or knew the region.

The one determining factor in breaking the case was the fraudster’s email address. This was the only piece of information that had to be real, since it was needed it to activate the account

It was a Gmail account, and after some investigation, it was discovered that the person was indeed from Ikeja.

The experts were able to identify the person as the owner of a shipping company in Nigeria. He was stealing the credentials to get information out of those companies with details of real oil cargo manifests. He intended to use that documentation to show it as a proof of product to the victims that he will try to scam.

The shipping companies infected by this malware are all around the world, but most of them were in Europe. The difficulty is that some of the companies have been hesitant to come

forward because 1) they were breached and information was copied, but there wasn't sufficient damage done, and more likely, 2) they were afraid their brand would be damaged for being involved in a fraud case.

As long as the Internet exists, people will try to scam the system, whether it's in the banking, financial services or even oil industries. As the Internet continues to evolve, old scams will be given new life, and new scams will pop up left and right. Unfortunately, the oil industry example is just one in a long line of Internet attacks we will continue to see, but with thorough investigation and a detection of patterns and missteps on the part of the cybercriminal, we will hopefully continue to gain traction in lessening the huge impact these scams have.

About the Author

Luis Corrons has been working in the security industry for more than 15 years, specifically in the antivirus field. He is the Technical Director at PandaLabs, the malware research lab at Panda Security. Luis is a WildList reporter, member of the Board of Directors at AMTSO (Anti-Malware Testing Standards Organization) and member of the Board of Directors at MUTE (Malicious URLs Tracking and Exchange). He is also a top rated industry speaker at events like Virus Bulletin, HackInTheBox, APWG, Security BSides, etc. Luis also serves as liaison between Panda Security and law enforcement agencies, and has helped in a number of cyber-criminal investigations.

INFOSEC WORLD 2015

Conference & Expo

March 23-25, 2015 | Disney's Contemporary Resort | Orlando, FL
Bonus Workshops March 21-22, 25-27

Cyber Defense Magazine readers save 10%!

Register with discount code **OS15/CDM** and save **10% off the main conference pass.**
Call MISTI Customer Service today to secure your spot **508-879-7999 ext. 501**

WWW.MISTI.COM/INFOSECWORLD

Assessing and Profiling the Insider Threats in Information Technology

By Dr. Joshua Sinai

The threat of insiders with malicious intent in a position of trust with access to critical aspects of an organization's Information Technology (IT) network, whether in government, the military, or the private sector has become a paramount concern. One reason for the escalation in this threat in the recent period is the massive and exponential explosion of available proprietary or classified information within organizations and the relative ease of access by what are presumed to be "trusted" IT professionals, ranging from data entry clerks to IT network administrators, with a minority of such individuals seeking to appropriate such sensitive information for their own political purposes.

Following several high profile cases of break-ins by such maliciously-intent insiders – particularly by Bradley Manning and Edward Snowden – cyber security practitioners are focused on deriving lessons from such breaches in order to prevent such penetration and exposure of their organizations' classified IT systems from recurring.

In retrospect, however, these incidents – with Manning's penetration reportedly occurring in 2009 and Snowden's in mid-2013 – could have been prevented at their earliest pre-incident phases had an equally serious case of inside penetration of a military's classified information system that had occurred in Israel in mid-2007 been more widely publicized, thereby alerting other nations' militaries that their classified information systems were vulnerable to insider exploitation by similarly disgruntled employees.

Anat Kamm – The First High Profile Insider Threat in IT

In the Israeli case, in mid-2007 20-year-old Anat Kamm, who was in the final phase of completing her compulsory two-year military service as assistant to the head of the bureau of Major General Yair Naveh, then the head of the Israel Defense Forces' (IDF) Central Command (which has responsibility for military operations in the West Bank), proceeded to surreptitiously download and copy onto a USB storage device an estimated 2,000 classified documents from several computers in the bureau, of which some 700 were "classified" or "top secret."[i]

In addition to the classified documents on targeted killings by Israel against suspected Palestinian terrorists – reportedly the focus of Kamm's "outrage" as a self-professed whistleblower – these also included an indiscriminate collection of documents on numerous other subjects, such as details of a planned invasion of Gaza, which was eventually launched in December 2008.[ii]

Yuval Diskin, at the time the head of the General Security Service (GSS) (also known as Shin Bet), charged that the case "had the potential to cause grave damage to state security" because

the documents were "the kind that any intelligence agency would be delighted to get its hands on."[iii]

After completing her military service in June 2007,[iv] it is reported that in September 2008 Kamm provided Uri Blau, an investigative journalist at the *Haaretz* newspaper, who specialized in military affairs, the USB thumb drive containing the downloaded classified documents and told him "I hope you'll know what to do with this."[v]

After reviewing the classified documents, Blau proceeded to publish two articles in *Ha'aretz* in November and December 2008, respectively, detailing the secret IDF meetings in which targeted killings were authorized for operations that were supposed to be arrest-based – but not deliberate killing – raids of Palestinian suspects. One of the articles also included a photo of the actual IDF documents Kamm had provided him.

Although, in accordance with Israeli law, Blau had submitted the articles to the office of the newspaper's military censor, which cleared them for publication, following the articles' publication, in early 2009, the IDF's investigators initiated an inquiry into the documents' leakage. After obtaining their respective phone records, and determining they had been in contact, Kamm was interrogated by the General Security Service of Israel (GSS – also known as Shin Bet), and reportedly confessed to leaking the documents, which is considered an act of treason since under Israeli law providing classified documents to a journalist is as treasonous as providing them to a terrorist group or foreign government.[vi]

Following a period of house arrest, in December 2009 Kamm was subsequently arrested and indicted on two counts of "serious espionage" – one for "gathering" and the other for "divulging" classified information, "with the intent to damage the security of the state."[vii] Kamm was subsequently sentenced to four and a half years imprisonment on charges of leaking classified material, and, as part of her plea deal, was early released from prison in late January 2014.

Profiling the Characteristics of "Insiders" in IT Threats

Similar to the radicalization processes that drive what are considered homegrown Western individuals into extremism and terrorism, risky insiders in IT, such as Kamm, Manning and Snowden – who are mostly lone wolves (although Manning and Snowden reportedly were linked to some degree with extremist hacktivist groups) – are radicalized by their own version of extremist ideologies.

In fact, just as Islamist "jihadism" became the new ideological fad in the 1980s to replace the previous far-left radicalism for those disaffected in the 1960s and 1970s, this new IT-based extremist ideology promotes the notion that all information, ranging from the most secret and proprietary to fee-based subscriptions to information carriers such as newspapers and music companies – should be free and accessible to everyone.

As demonstrated by the cases of Kamm, Manning and Snowden, such "radicalized" individuals feel an overwhelming disgruntlement and anger towards their governments and their national

security programs. They appear to have a highly narcissistic and inflated sense of themselves that they are "above the rules" of their respective organizations, and they have a strong desire to draw worldwide attention to themselves by carrying out a grandiose act of defiance against their employers. In terms of risky behavioral indicators, they appear to be isolated and alienated from their co-workers (although, due to the sensitive nature of her employment, the relations between Kamm and her military service co-workers are not publicly known).

While Manning and Snowden surreptitiously downloaded classified documents, and engaged in suspicious foreign contacts with extremist activist leaders (such as, in the case of Manning, with Julian Assange, while Snowden had been in contact with Glenn Greenwald, an activist journalist with *The Guardian* newspaper), Kamm was more discreet and only contacted what she believed was a trusted and responsible Israeli newspaper reporter. These – and, surely, numerous other – personal and behavioral risk indicators appeared to drive them to take revenge and retaliation by leaking classified information about their government's covert national security programs.

It should be pointed out that while some of the secret and proprietary documents that are posted in sites such as *WikiLeaks* may also be generated by such insiders, many of these documents are also generated from hacktivists belonging to groups such as LulzSec and Anonymous who surreptitiously penetrate their targeted organizations to obtain such sensitive documents to advance their own political agendas (as opposed to profiting financially from such exposures).

Conclusion: Preemptively Preventing Information Technology Insider Threats

To preemptively identify a susceptible individual in an organization who appears to be on a trajectory to becoming an insider threat in information technology, it is crucial for security professionals to develop a situational awareness of the potentially risky personal and behavioral characteristics that such individuals exhibit in their daily work activities.

Such situational awareness also requires understanding the psychological and behavioral profiles of such individuals who progress along such insider threat trajectories in order to preempt them at their workplace at the earliest possible pre-incident phases.

A comprehensive series of preventative internal security measures were reportedly implemented by the IDF following Kamm's breach incident, such as increased use of lie-detector tests for soldiers with access to classified information and internal warning flags raised when any deviation from normal activity from one's computer terminal in an IT network takes place.[viii]

It is not known, however, whether these types of preventative measures were shared at the time with the counterintelligence departments of Israel's allied partners, particularly the United States, in order to prevent the types of breaches that were later on carried out by Manning and Snowden.

While Western governments are implementing stricter access control measures to deter susceptible employees from becoming insider threats to their organizations' proprietary and

classified information technology systems, the insider threat is likely to persist due to the ever-increasing proliferation of anti-secrecy militant groups within the information technology community who seek to advance their own political agendas.

About the Author

Dr. Joshua Sinai is a Director of Analytics & Business Intelligence at the Resilient Corporation (www.resilient.com) and at its wholly-owned subsidiary, CRA (www.cra-usa.net), where he specializes in terrorism, counterterrorism, and homeland security studies. He has worked as an Associate Professor/Research at VT Research Center - Arlington, Virginia Tech (National Capital Region), which he joined in April 2010. Dr. Sinai's specializations include developing methodologies to forecast terrorist warfare, root cause analysis, performance metrics in counterterrorism, and insider threats in IT. He has more than 25 years of experience in government (including working at Department of Homeland Security's Science & Technology Directorate and, as a contractor, at a U.S. government counterterrorism operations center). Dr. Sinai has published a pocket handbook on active shooter prevention and more than 80 articles and book reviews on terrorism and counterterrorism related topics, in academic publications, magazines, and newspapers. He also serves as Book Reviews Editor for the online academic journal "Perspectives on Terrorism," for which he also writes the regularly published "Counterterrorism Bookshelf" review column. He holds a Ph.D. in Political Science, with a specialization in Comparative Politics and the Middle East, from Columbia University.

American Conference Institute's
15th Advanced Global Legal & Compliance Forum on

Cyber Security & Data Privacy and Protection

Inquire about in-house, government, and group rates

January 15–16, 2015 | Washington Plaza Hotel | Washington, DC

Pre-Conference (early a.m.) Workshop – January 15 • Post-Conference (p.m.) Workshop – January 16

Earn CLE Credits

Featured Speakers From:

FTC
U.S. DHS
FBI
NIST
U.S. EEOC
U.S. DOJ
U.S. CFTC
California DOJ
Missouri AG Office
Vermont Office of the AG
Illinois Office of the AG
Pennsylvania Office of the AG
MA Consumer Affairs and Business Regulation
TX Comptroller of Public Accounts
Interactive Advertising Bureau
Network Advertising Initiative

Be sure to also book for Workshops A and B:

A Privacy & Security 101

B Fundamentals of Cyber & Data Risk Insurance

This conference is approved for CPE credits, as an Approved Privacy Education Provider and Activity.

Sessions Include:

- Federal Regulatory, Legislative, and Enforcement Landscape: Changes on the Horizon and Integrating New and Anticipated Initiatives Into Your Privacy and Compliance Program
- Unique Regulatory and Enforcement Insights by State Attorneys General and Consumer Protection Agencies on Emerging Privacy Initiatives, Settlement and Enforcement Trends, Security Breach Notification Requirements, and More
- INTERNATIONAL: Managing a Global Privacy Program and Preparing, Collecting, Using and Transferring Data Across Borders
- The Intersection of Healthcare and Data Security: OCR, HHS, and HIPAA Cyber Security and Data Privacy and Protection
- The Internet of Things: Privacy, Security, New Risks and Developing Threats
- Practicing Privacy by Design: Ensuring Cyber Security and Data Privacy & Protection Don't Become an Afterthought
- Cyber Security Preparedness: Best Practices for Data Breach Incident Response Teams With a Focus on Preemptive Measures to Take and Rehabilitating Your Image
- The Cloud: Best Practices on Third-Party Vendor Compliance and Negotiating Terms of Cloud Services Contracts and Service Level Agreements
- Privacy on Mobile Platforms and Privacy Disclosures for Mobile Apps: Best Compliance Practices
- Ensuring Compliance With Privacy Requirements for Online Behavioral Advertising and Marketing Initiatives: Cookies, "Do-Not-Track", and Other Behavioral Targeting Nuances
- Big Data in the Cyber Security and Privacy Protection Context: Aggregating Data, Data Analytics, Data Mining, and Privacy Rights
- Class Actions & Litigation Roundup: Recent Data Breach Cases, Mega Privacy Actions, TCPA and Texting Suits, and Assessing What Claims Are Worth

Conference Co-Chairs

Russell Schrader
Visa, Inc.

Ashley Taylor, Jr.
Troutman Sanders LLP

as well as:

Prudential Financial
McKesson Corporation
NeuStar, Inc.
Motorola Mobility
Epsilon
GE Healthcare
Farmers Group, Inc.
SCOR Reinsurance Company
Northwestern Mutual
KAYAK Software Corporation
Marriott International
Hewlett-Packard Company
W.R. Grace
BNY Mellon
PPD
The Coca-Cola Company
Viewpost
Microsoft
PrizeLogic
Google
Freedom Specialty Insurance Co.
Condé Nast
Advocate Health Care
University Hospitals
Foursquare Labs, Inc.
AIG
IBM
Avon
Nationwide
AppNexus
Unum
Wyndham Worldwide

Register Now | 888-224-2480 | AmericanConference.com/Privacy

Subscribers are entitled to $200 off registration with Discount Code: CDM200

DDoS Out in Full Force

By Todd Weller, VP, Corporate Development, Hexis Cyber Solutions

Distributed Denial of Service (DDoS) attacks are on the rise and here to stay. Experts theorize that this is due in large part to the easy access in obtaining one of these malware toolkits. Sophisticated DDoS attacks are only going to get worse, so what should companies do to best prepare themselves?

Let's take an example from one of the companies that experienced a DDoS attack this past year, Sony PlayStation. Sony's PlayStation and Entertainment Networks were taken down via a DDoS attack, however, according to Sony's official blog post issued following the attack, no customer or corporate data was leaked or compromised.

This wasn't the first time the Japanese electronics company has been under the firing squad. In spring of 2011, Sony suffered a massive breach against its video game online network that ultimately led to the theft of names, addresses and even credit card data of almost 77 million user accounts.

At the time, this attack was considered one of the largest-ever Internet security break-ins. In comparing these two instances, it looks like Sony learned its lesson when it comes to disclosing the news in a timely manner. Back in 2011, the company waited 7 full days until announcing the incident; this time around, Sony made a public statement immediately following the attack.

In addition to the network being taken down, the hacking group responsible, Lizard Squad, is also claiming to be behind the plane incident involving Sony Online Entertainment President, John Smedley in which the executive's American Airlines flight to San Diego had to be diverted based on a looming bomb threat. This raises an interesting question – what were Lizard Squad's driving motives behind the attack? Were these two isolated incidences or was there a larger connection?

Organizations across all industries should take a page from Sony's lesson book; recognizing that an attack has been successfully executed and later publicly disclosing the (known) details of the incident is the first step in adequately handling the aftermath of a breach.

The next step should include an in-depth analysis of how the attackers able to execute the breach on hand; in doing so, organizations can collect the necessary information they need to make efficient decisions on prevention of future similar incidences. If you're interested in learning more about to do after an attack, check out the Hexis eGuide, "5 Things to Do After You've Been Hacked."

It's clear to speculate that because these breaches are happening over and over again, companies need to have the right tools in place to better protect themselves. Remember – it's no longer a matter of if you've been attacked, but when you're going to be attacked.

About the Author

Todd Weller, VP, Corporate Development, joined Hexis Cyber Solutions in March 2014. His responsibilities include analyst relations, competitive and market intelligence, corporate visibility, M&A, and strategic partnership development. Todd draws on his 17+ years of experience as an equity research analyst where he covered the security industry for much of that time. In his equity research career Todd provided research coverage of over 60 companies across several technology sectors, including security, infrastructure software, data center/cloud hosting, and healthcare IT.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

The Anatomy of a Social Media Cyber Attack

How Social Media Makes Cyber Security Attacks Bigger, Badder, and More Effective

Evan Blair, Chief Operating Officer, ZeroFOX

Social media has forever changed how we interact. Three out of four internet connected people are on social, totaling nearly 3 billion accounts among Facebook, Twitter and LinkedIn alone. It has created a close-knit internet community, altered how businesses develop and facilitates global conversation. But social is as vulnerable as it is powerful. Cybercriminals exploit this unprecedented internet connectivity to target organizations via their brand, employees and customers. From a cyber criminal's perspective, the scale of social media makes it the simplest and lowest-cost method to target organizations. According to Norton, 4 out of 10 people have fallen victim to cybercrime on social media.

Social media cyber attacks come in a variety of forms. Social networks, despite their best intentions and security measures, provide a fresh avenue for oldest-trick-in-the-book attacks, like phishing and drive-by malware downloads. Using social media increases the scope and efficacy of an attack while dramatically lowering the cost and effort of execution. Unlike email, social media goes unmonitored by an organization's existing security framework, allowing hackers to strike an organization's people from top to bottom without ever tripping the network alarms.

Hackers often leverage botnets to assist with social media-based cyber attacks. A botnet is a collection of automated accounts that work in tandem to replicate the actions of the hacker-operated "bot-head." To amplify and sharpen attacks, botnets engage in widespread trendjacking or hashtag hijacking. Trendjacking or hashtag hijacking is the tactic of appending unrelated hashtags to a post to capitalize on a trend or to target a specific audience. Doing so amplifies the attack to the largest or most susceptible populations.

Bot accounts are often filled with attractive, funny or otherwise eye-catching photos. They will connect with an organization's affiliates to seem more legitimate, a tactic known as "gatekeeper friending." Bots post randomly throughout the day to seem more human and disguise malicious links by interspersing them with canned book quotes, algorithmically generated strings of words or benign links. This also helps them fly under the radar of social networks' Terms of Service, which prohibit such accounts.

Automated accounts are not always malicious--many are used to simply retweet the weather or the news. But some are more spammy. Creating botnets offers a hacker a couple options for making a quick dollar. After a botnet builds up a base of followers, online marketers will pay to have their content posted via the botnet reaching, in some cases, hundreds of thousands of users. This is a common practice for cheap advertising and spam. Those controlling the botnet can also sell, or "flip," the head account. People pay top dollar for an account with a large prebuilt following.

Online marketing and account flipping is a fairly innocuous use of a botnet. The bigger risk is the spread of malicious links. With a botnet in place and a foundation of unmonitored posts, a hacker has created a strong foundation from which to launch a phishing or malware distribution campaign. Hackers will build a fake landing page and share the link via the botnet. This type of phishing scheme often mimics a commonly used support or customer service hashtag for an enterprise, thus targeting the company's customers. Malware distributed on social, which comes in a host of different shapes and sizes, can compromise an organization's network, install malicious applications or steal sensitive data.

BYOD (Bring Your Own Device) culture magnifies social media security risks. If any device infected from a social account accesses the organization's network, malware can steal information from anywhere in the enterprise. Social media is the fastest growing threat vector on the internet – expect it to take the front seat of cyber security conversations in the coming years.

The illegal use of social media not only makes the cyber criminal's job easier, but makes the security professional's job much harder. Bots are difficult to detect and bypass traditional security measures. Other cyber attacks on social media are even more difficult to detect, such as social engineering, impersonations, and fraud. "Soft hacks" are rampant on social, yet are some of the most dangerous. Security solutions must adapt to alert on soft indicators of compromise in order to combat this growing threat vector.

As social media continues to grow, cyber security must grow with it.

About the Author

Evan Blair is the Co-Founder and Chief Operating Officer at ZeroFOX. Evan is responsible for driving the corporate vision through execution-focused initiatives as well as business development and marketing. He was integral in securing the companies $11M Series A investment, winning the SINET 16 Innovator award and serving as security thought leader, having spoken at industry conferences in Las Vegas, Washington DC, New York, Baltimore and San Francisco. Prior to that, Evan was a member of the Accuvant Leadership Team where he led the multi-million dollar Partner Solutions practice. At the time of his departure, Accuvant was the 2nd largest privately held cyber security solutions provider, had recognized over $1 billion in revenue since inception, and had capabilities with over 175 global partners. In 2008, Evan joined Foster at Baltimore-based cyber start-up Ciphent, where he was responsible for executing the marketing and sales strategy for the organization. Charged with the ultimate goals of increasing sales, profitability, and revenue, Evan's department supported the company's three-year revenue growth rate of nearly 1000%. Previously, Evan held financial and business development roles at Application Security Inc. He began his career as a financial analyst with Dresdner Kleinwort in Manhattan, NY and holds a BA in Economics from Wake Forest University.

How to Avoid Incorrectly Labeling Innocent Customers as Guilty this Holiday Shopping Season

By Reed Taussig, president and CEO, ThreatMetrix

The holiday shopping season is under way with two of the year's largest shopping days – Black Friday and Cyber Monday – taking place in November. Consumers are projected to spend a record $600 billion this holiday shopping season. Hand-in-hand with an increase in consumer spending is the annual monsoon of increased online credit card theft, identity theft and attempted bank fraud. It is a predictable annual feeding frenzy that will come on top of an already record year of significant wins for global cybercriminals.

All too often, Target, Home Depot, eBay and other major retailers are portrayed as the culprits behind the rapid increase in cybercrime following recent data breaches when in fact retailers, just as consumers, are the victims of the arms race between enterprise security and fraud departments and the well-funded, successful, cyber thieves.

As cybercrime becomes more advanced, retailers, financial services companies and enterprises continuously develop more advanced ways to protect sensitive information from being compromised or being used once the company has been breached. Advanced fraud prevention strategies are certainly justified and necessary, but the unfortunate side effect is that online consumers are often **presumed to be guilty until proven innocent** during the online shopping experience.

The net result of incorrectly assuming customers are guilty has been a rapid increase in the use of two-factor authentication and out-of-band authentication, which is expensive to the enterprise and introduces many extra steps and a lot of inconvenience into the online shopping experience. This in turn increases shopping cart abandonment rates, leading to reduced topline revenue for the business.

Businesses are justified in adding layered security measures, especially when the percentage of risky or fraudulent transactions is taken into consideration. The following data from the ThreatMetrix® Global Trust Intelligence Network reveals several stats about online fraud percentages:

- As many as **10 percent** of all online credit card applications are executed using either stolen or synthetic identities
- On average as many as **five percent** of all online credit card purchases across industries are suspicious or outright fraudulent and for some industries this number is double or even triple that average
- To put this into perspective, ThreatMetrix processes close to one billion online transactions per month and of these, more than fifty million will be either suspicious, triggering additional costly and inconvenient additional screening measures, or outright fraudulent.

While these fraud statistics are significant and can lead to vast financial losses without preventative measures in place, online channel friction, or in other terms customer harassment, can be just as detrimental to the bottom line.

Such friction leads to lost revenues due to increased but necessary security measures resulting unintended consequence of combating global cyber-terrorists.

Passive, context-based authentication based on shared global intelligence is a much more effective way to proactively authenticate customers without arduous step-up authentication. Rather than interrupting the customer experience with an out-of-band SMS message or direct telephone call, which absolutely will impact retailers' and other businesses' top line revenue and reduce customer satisfaction, businesses can now passively identify and authenticate each online customer based on the recent experiences of thousands of other enterprise companies who have successfully conducted online transactions with that customer.

Such technology can reduce your use of step-up and out-of-band authentications by as much as 70 percent with no increase in fraud, therefore greatly improving both the bottom line and the customer experience.

Passive context-based authentication using global shared intelligence is completely transparent to the customer experience, can be processed in real time and costs less than a penny per transaction. It also provides much broader and better security than businesses currently receive from proactive, customer-disruptive solutions.

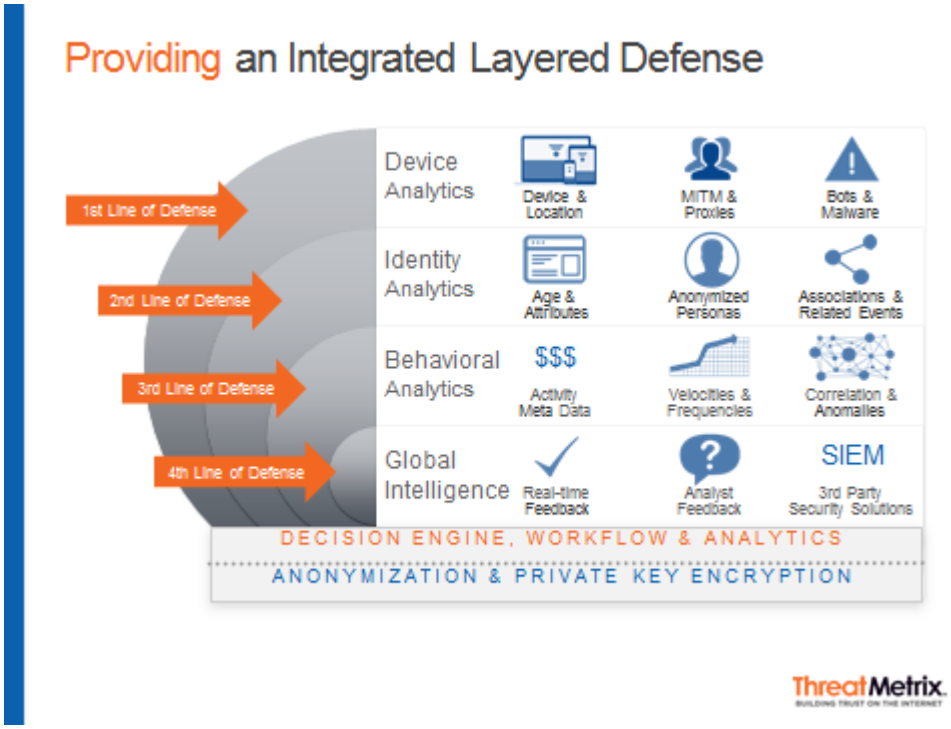
Context based authentication includes the detection of malware, hidden proxies, the history, number and velocity of user credentials, and customers' actual behavior.

ThreatMetrix passive authentication uses four layers of defense to identify in real time good customers and criminal actors. These include:

- **Device Analytics** examine the attributes, location and reputation of a customer's endpoint device regardless of whether it is a desktop or mobile device. Such analytics identify whether or not that device is behind a hidden proxy or unregistered VPN, determine whether that device has been infected with malware such as a Man-in-the-Browser (MitB) Trojan and informs the business whether or not that customer is using private browsing to hide their true identity.
- **Identity Analytics** informs the business about related devices and user credentials an individual customer regularly uses (this capability precludes the use of more invasive forms of two-factor authentication simply because a customer elected to use a different device), and the authenticity of a customer's credentials (for example, shipping and billing addresses).
- **Behavioral Analytics** correlate related events and customer activities across e-commerce, financial services and enterprise customer-facing websites around the world. Rather than proactively calling that customer and interrupting thee online experience, behavioral analytics deliver to you the meta history of each consumer so businesses can

passively and instantly authenticate that person without any customer involvement required.

- **Global Intelligence** provides the tools to analyze transactional results and trends, manage rules and risk levels that are unique to each company's business and to integrate other third-party solutions.



Of equal importance to a seamless customer experience, ThreatMetrix provides advanced fraud prevention and context-based authentication without the need to expose the true identity customers, therefore protecting businesses you from the ever increasing list of confusing and conflicting privacy laws and regulations.

The holiday shopping season should be a time for increased revenue opportunities for retailers and other businesses, but to capitalize on increased spending, businesses need advanced cybersecurity solutions to protect against ever increasing cybersecurity threats.

Context-based authentication and global network intelligence can dramatically improve e-commerce security during the holidays and year round without a negative impact on the overall customer experience.

About the Author

Reed Taussig has more than 30 years of experience in the computer hardware and software fields. Prior to ThreatMetrix™, Mr. Taussig was president and CEO of Vormetric, Inc., a leader in data privacy and protection. Under his leadership, Vormetric established itself as a leading provider of encryption solutions for the Payment Card Industry Data Security Standards industry.

Mr. Taussig also served as president and CEO of Callidus Software (NASDAQ: CALD), the leading provider of enterprise incentive compensation management application systems. As founding CEO and the fifth employee, Mr. Taussig led the growth of company to more than $70 million in revenues and over 350 employees.

Prior to Callidus Mr. Taussig was the president and CEO of inquiry.com, a pioneer in the B2B Internet space as well as senior vice president of operations for Gupta Technologies, the leader for PC client server software development tools and databases. Mr. Taussig holds a bachelor of arts degree in economics from the University of Arizona.

Verizon's Supercookies and using a VPN as Defense

In a new form of online user tracking, Verizon have confirmed that they have been uniquely identifying their wireless users to advertisers for the last two years using so called supercookies.

Privacy Compromised

In a process first described by privacy group Electronic Frontier Foundation, supercookies, or perma-cookies as they've also been coined, involve directly changing the HTTP request between the client and server platforms. Verizon is the US's most used mobile data provider and has been rewriting the headers of all HTTP requests from non-business and government users on their wireless network.

By injecting a custom header titled X-UIDH with a unique identifier, Verizon then allows a paid API call to get a profile linked to that identifier. In this way websites can effectively track the entire non encrypted browsing history for any given Verizon user.

Since the process takes place at the network level after the request has left the requesting device, do-not-follow-me, anti-cookie software, and private browser tabs will do nothing to combat the privacy concerns that have left many Verizon's users reeling.

The primary privacy issue with this tracking technique is that every single website, not just selected Verizon partners, can view this header without anyone knowing they are doing it. All the data the website owners need to start building a permanent profile of a user is right there in the HTTP request.

In a conversation with Verizon Kashmir Hill, writer for Forbes, the mobile giant confirmed that the system had been running for "two years". Given that amount of time, Senior Verizon privacy officer Kathy Zanowic said she was "surprised" by the attention the story had got. Kashmir also spoke to AT&T who confirmed that they had a similar system "in testing" for "a little while".

The Wider Moral and Legal Issues

It's clear that more people, especially Verizon's own customers, are now picking up on this issue. "It's gone relatively unremarked by the security, privacy, and broader technical community, in part, because it's so hard to observe," says Jacob Hoffman-Andrews of the Electronic Frontier Foundation.

As debate moves from initial anger to more analytical nature, the central question, one of the overarching morality and legality of this new form of ISP intervention has been raised. While it is

not uncommon for paid services to also then sell customer data to selected third parties, to do so without having full and frank disclosure is harder to take for consumers.

A clear and easy to find “opt out” is also normally expected. While Verizon does provide this opt-out, is does not actually stop the injection from taking place, only the building of your unique profile. In other words, you are still being tracked, but websites have to build their own profiles of you.

Legally too, Verizon may be on shaky ground too. The Communications Act prohibits carriers from giving up identifying information regarding their customers, or providing others with the mean to do so. This is at the core of a possible lawsuit or action, said Nate Cardozo a lawyer for the Electronic Frontier Foundation. Other legalities are also flagged up by the Federal Wiretap Act. This Act is designed to stop personal communications being changed when data is transmitted (without an attendant court or consent).

VPNs to the Rescue

Both the Electronic Frontier Foundation and private security specialists were quick to provide a way round the Super Cookie; encryption. Since encrypted traffic cannot be altered so easily by network carriers, using a Virtual Private Network offers an effective means to stop the header injection.

While nearly all operating systems now have inbuilt VPN clients, the Verizon injection takes place on their mobile network (no reports of this same tracking technique have been made for the Verizon broadband network). This means that you need to form a VPN on your smartphone or tablet; a far from easy or convenient proposition.

Use of the TOR network can also circumnavigate the problem. While you may be able to use TOR on your mobile, most current implementations are difficult to use. In addition to this both TOR and VPN will add at least some performance degradation to your connection. In the case of using a commercial VPN provider there will also be additional cost.

About the Author

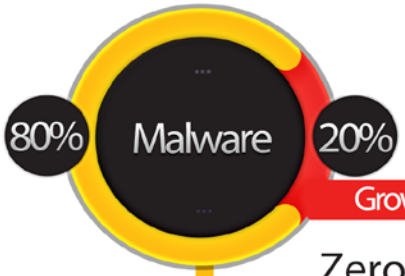
Patrick Lincoln is founder of Unified Communications Company Solution IP, which he set up in 2006. An authority in the industry, he spent many of his formative years building relationships within the telecoms community in the South West of England. You can connect with Solution IP on Twitter or Facebook.

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 ™

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

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

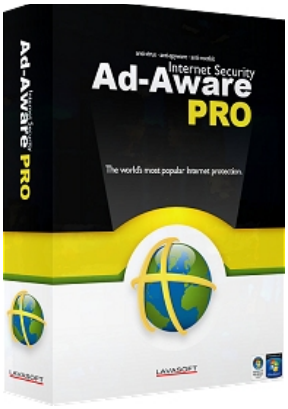
So use it by going here:

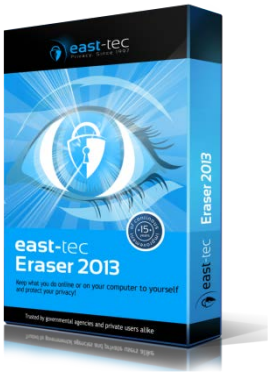
http://www.naisg.org/techtips.asp

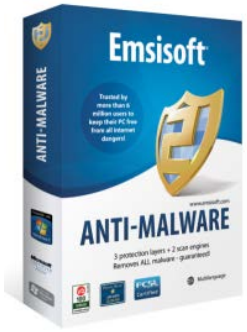
SOURCES: CDM and NAISG.ORG

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

http://register.cyberdefensemagazine.com







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

Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine November 2014

Sample Sponsors:

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

Cyber Warnings Newsflash for November 2014

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…

FBI Chief Comey Hints At Phone Encryption Regulations Suggesting The Pendulum Of Privacy Has 'Swung Too Far'
http://www.idigitaltimes.com/fbi-chief-comey-hints-phone-encryption-regulations-suggesting-pendulum-privacy-has-swung-too-far

Fighting the Globalization of Cybercrime
http://www.bankinfosecurity.com/interviews/fighting-globalization-cybercrime-i-2480

New attack hides stealthy Android malware in images
http://www.pcworld.com/article/2835432/new-technique-allows-attackers-to-hide-stealthy-android-malware-in-images.html

Recognizing Evasive Behaviors Seen as Key to Detecting Advanced Malware
http://threatpost.com/recognizing-evasive-behaviors-seen-as-key-to-detecting-advanced-malware/108888

Utterly crazy hack uses long-distance lasers to send malware commands via all-in-one printers
http://www.pcworld.com/article/2834972/allinone-printers-can-be-used-to-control-infected-airgapped-systems-from-far-away.html

Hordes of cable modems, Web cams, printers can become DDoS launch platforms
http://www.networkworld.com/article/2834916/security0/hordes-of-cable-modems-web-cams-printers-can-become-ddos-launch-platforms.html

Clapper worries about cyber threat from Russia
http://thehill.com/policy/technology/221065-clapper-worries-about-cyber-threat-from-russia

NSA chief: 1,000 new jobs coming to S.A.

http://www.mysanantonio.com/business/local/article/Cyber-commander-says-1-000-new-jobs-coming-to-S-A-5827450.php

Pentagon Needs to Build Cybersecurity into the Acquisition Process
http://www.nextgov.com/cybersecurity/2014/10/pentagon-needs-build-cybersecurity-acquisition-process/96461/

Mastercard launches first thumbprint biometric card
http://www.theguardian.com/money/2014/oct/17/mastercard-thumbprint-biometric-card

China says US must change 'mistaken policies' before deal on cyber security
http://www.theguardian.com/world/2014/oct/19/china-cyber-security-cooperation-problematic-mistaken-us-policies

'Crypto wars' return to Congress
http://thehill.com/policy/cybersecurity/221147-crypto-wars-return-to-congress

U.S. Data Breach Notification Law Unlikely in 2014
http://www.govinfosecurity.com/us-data-breach-notification-law-unlikely-in-2014-a-7453

Infographic: A brief history of malware
http://net-security.org/malware_news.php?id=2886

Whisper chief executive answers privacy revelations: 'We're not infallible'
http://www.theguardian.com/world/2014/oct/19/-sp-whisper-chief-executive-on-privacy-revelations-were-not-infallible

Spike in Malware Attacks on Aging ATMs
http://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/

Dropbox used for convincing phishing attack
http://www.computerworld.com/article/2835166/dropbox-used-for-convincing-phishing-attack.html

World's Top Privacy Experts Worry About Internet Of Things
http://www.forbes.com/sites/adamtanner/2014/10/20/worlds-top-privacy-experts-worry-about-internet-of-things/

Defending Against Government Intrusions
http://www.govinfosecurity.com/defending-against-government-intrusions-a-7452

Feds urge early cooperation in malware investigations
http://fcw.com/articles/2014/10/20/cyber-resiliency-from-cooperation.aspx

Chip-and-PIN increases cybersecurity
http://thehill.com/blogs/congress-blog/technology/221113-chip-and-pin-increases-cybersecurity

U.S. national security prosecutors shift focus from spies to cyber
http://www.reuters.com/article/2014/10/21/us-usa-justice-cybersecurity-idUSKCN0IA0BM20141021

As cybercrime goes global, it's getting costlier
http://www.cbsnews.com/news/cybercrime-goes-global-gets-costlier/

Hacking ATMs: No Malware Required
http://www.govinfosecurity.com/hacking-atms-no-malware-required-a-7460

Why You Shouldn't Count On General Liability To Cover Cyber Risk
http://www.darkreading.com/why-you-shouldnt-count-on-general-liability-to-cover-cyber-risk/d/d-id/1316758

Cyber demand leaves states at risk
http://thehill.com/policy/cybersecurity/221320-cyber-demand-leaves-states-at-risk

Chinese state accused of attacking Apple's iCloud
http://www.theguardian.com/technology/2014/oct/20/chinese-state-accused-attacking-apple-icloud

EFF, Snowden Dispute FBI Claims on Device Encryption
http://threatpost.com/eff-snowden-dispute-fbi-claims-on-device-encryption/108931

Staples customers likely the latest victims of credit card breach
http://net-security.org/secworld.php?id=17518

China suspected of cyberattack on Apple
http://thehill.com/policy/cybersecurity/221435-chinese-government-suspected-of-launching-apple-cyberattack

US Justice Dept. focuses new squad on cybercrime combat
http://www.networkworld.com/article/2836310/security0/us-justice-dept-focuses-new-squad-on-cybercrime-combat.html

Former NSA chief on cyber attacks: 'We've got to work together'
http://fortune.com/2014/10/21/keith-alexander-cyber-security/

Former NSA Official: Here Are 4 Things Edward Snowden Gets Wildly Wrong About American Spying

http://www.businessinsider.com/expert-here-are-4-things-edward-snowden-gets-wildly-wrong-about-the-nsa-2014-10

DOJ's National Security Division Reorganizes for Cyber and Corporate Espionage Threats
http://www.mainjustice.com/2014/10/21/dojs-national-security-division-reorganizes-for-cyber-and-corporate-espionage-threats/

U.S. government probes medical devices for possible cyber flaws
http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022

Malware directs stolen documents to Google Drive
http://net-security.org/malware_news.php?id=2888

Windows Warning: Zero-Day Attack
http://www.govinfosecurity.com/windows-warning-zero-day-attack-a-7466

D.C.'s Complicated View of Cyberwar, Regulation, Liability
http://threatpost.com/d-c-s-complicated-view-of-cyberwar-regulation-liability/108954

Espionage Hacks Tied to Russians
http://www.govinfosecurity.com/espionage-hacks-tied-to-russians-a-7487

Leader of "most sophisticated cybercrime ring" sentenced to 11 years
http://arstechnica.com/tech-policy/2014/10/leader-of-most-sophisticated-cybercrime-rings-sentenced-to-11-years/

Tor users advised to check their computers for malware
http://www.theguardian.com/technology/2014/oct/28/tor-users-advised-check-computers-malware

Zero-day in Samsung 'Find My Mobile' service allows attacker to remotely lock phone
http://www.computerworld.com/article/2839240/zero-day-in-samsung-find-my-mobile-service-allows-attacker-to-remotely-lock-phone.html

Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation
http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation

Shellshock Exploits Targeting SMTP Servers at Webhosts
http://threatpost.com/shellshock-exploits-targeting-smtp-servers-at-webhosts/109034

Insurers fight to bar cyber coverage under commercial general liability policies
http://www.businessinsurance.com/article/20141026/NEWS07/141029850?tags=|299|329|76|303

NSA surveillance limits: Focus turns to courts
http://www.theherald-news.com/2014/10/28/nsa-surveillance-limits-focus-turns-to-courts/ar0sj44/

Researchers identify sophisticated Chinese cyberespionage group
http://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html

Crooks use stolen magnetic payment card info to make fraudulent chip-enabled transactions
http://net-security.org/secworld.php?id=17543

Hackers breach some White House computers
http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html

In cybersecurity battle, government-business cooperation necessary: Justice official
http://www.washingtontimes.com/news/2014/oct/28/in-cybersecurity-battle-government-business-cooper/

Hackers Are Using Gmail Drafts to Update Their Malware and Steal Data
http://www.wired.com/2014/10/hackers-using-gmail-drafts-update-malware-steal-data/

Security vendor coalition cleans 43,000 malware infections used for cyberespionage
http://www.pcworld.com/article/2839912/security-vendor-coalition-cleans-43000-malware-infections-used-for-cyberespionage.html

Cyberespionage: 'This Isn't a Problem That Can Be Solved'
http://threatpost.com/cyberespionage-this-isnt-a-problem-that-can-be-solved/109063

Cybersecurity: Why It's Not Just About Technology
http://www.governing.com/columns/smart-mgmt/col-cybersecurity-organizational-culture-risk-management.html

IT is losing the battle on security in the cloud
http://net-security.org/secworld.php?id=17546

BlackEnergy Malware Used in Attacks Against Industrial Control Systems
http://threatpost.com/blackenergy-malware-used-in-attacks-against-industrial-control-systems/109067

NIST Guide to Cyber Threat Information Sharing open for comments
http://net-security.org/secworld.php?id=17554

Police vs cartels in the high-tech battle to stop cybercrime
http://www.cnn.com/2014/10/30/tech/web/police-vs-cartels-cybercrime/

Carders offer malware with the human touch to defeat fraud detection

http://www.theregister.co.uk/2014/10/30/carders_flog_bankbeating_fraud_funnel/

Arrests made after 'specialist malware' used in £1.6 million ATM heist
https://nakedsecurity.sophos.com/2014/10/29/arrests-made-after-specialist-malware-used-in-1-6-million-atm-heist/

It came from the server room: Halloween tales of tech terror
http://arstechnica.com/information-technology/2014/10/it-came-from-the-server-room-halloween-tales-of-tech-terror/

Keep Calm & Verify: How To Spot A Fake Online Data Dump
http://www.darkreading.com/cloud/keep-calm-and-verify-how-to-spot-a-fake-online-data-dump/d/d-id/1317066

Major cyberattack coming, experts warn
http://thehill.com/policy/cybersecurity/222245-major-cyber-attack-coming-experts-warn

Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin
http://www.wired.com/2014/10/world_passport/

Biggest ever cyber security exercise in Europe is underway
http://net-security.org/secworld.php?id=17558

Popular Science Website Infected, Serving Malware

http://threatpost.com/popular-science-website-infected-serving-malware/109089

Cars, toasters, medical devices add to DHS's cyber headaches
http://www.federalnewsradio.com/473/3733484/Cars-toasters-medical-devices-add-to-DHSs-cyber-headaches

How NSA Director Wants to Build an IoT Security Coalition
http://www.eweek.com/security/how-nsa-director-wants-to-build-an-iot-security-coalition.html

Nato frontline in life-or-death war on cyber-terrorists
http://www.theguardian.com/world/2014/oct/30/nato-frontline-cyber-terrorists-war

Cybercrime genius jailed after £6.3m theft from RBS
http://www.express.co.uk/news/uk/529163/Cybercriminal-Sergei-Tsurikov-jailed-theft-RBS

Changing the Way We Fight Malware
http://securitywatch.pcmag.com/none/329047-changing-the-way-we-fight-malware

Beware of the malware walking dead
http://www.scmagazine.com/beware-of-the-malware-walking-dead/article/380336/

The Bill for Cybersecurity: $57,600 a Year
http://www.businessweek.com/articles/2014-10-31/cybersecurity-how-much-should-it-cost-your-small-business

Welcome To My Cyber Security Nightmare
http://www.darkreading.com/attacks-breaches/welcome-to-my-cyber-security-nightmare/a/d-id/1317079

The security threat of unsanctioned file sharing
http://net-security.org/secworld.php?id=17563

White House Hack: A Lesson Learned
http://www.govinfosecurity.com/interviews/white-house-hack-lesson-learned-i-2492

Doug Maughan: DHS to Key 2015 Cyber Funding Awards on Forensics, Remote Access
http://www.executivegov.com/2014/11/doug-maughan-dhs-to-key-2015-cyber-funding-awards-on-forensics-remote-access/

Report Links China to Cyberattacks on Hong Kong Protestors
http://time.com/3548754/hong-kong-protest-cybersecurity-hack/

Acting out: Cyber simulation exercises
http://www.scmagazine.com/acting-out-cyber-simulation-exercises/article/377716/

Researchers audit the TextSecure encrypted messaging app
http://net-security.org/secworld.php?id=17575

Cybercrime: the new normal
http://www.scmagazineuk.com/cybercrime-the-new-normal/article/378707/

Cyber security: Security awareness can't be just a one off

http://www.itpro.co.uk/security/23418/cyber-security-security-awareness-cant-be-just-a-one-off

Facebook embraces Tor users, sets up onion address
http://net-security.org/secworld.php?id=17574

An Unprecedented Look at Stuxnet, the World's First Digital Weapon
http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Security Contractor Breach Goes Unnoticed for Months

http://www.dailyfinance.com/2014/11/04/security-contractor-breach-goes-unnoticed-for-months/

Have E-ZPass? Watch out for slimy ASProx-based malware ploy
http://www.networkworld.com/article/2842773/security0/have-e-zpass-watch-out-for-slimy-asprox-based-malware-ploy.html

New version of Backoff detected, malware variant dubbed 'ROM'
http://www.scmagazine.com/new-version-of-backoff-detected-malware-variant-dubbed-rom/article/381054/

This system will self destruct: Crimeware gets powerful new functions
http://arstechnica.com/security/2014/11/this-system-will-self-destruct-crimeware-gets-powerful-new-functions/

Persistent cyberattacks of U.S. companies on the rise
http://www.washingtontimes.com/news/2014/nov/3/riley-walters-persistent-cyberattacks-on-us-compan/

NSA director says major hurdles hinder cybersecurity
http://www.usatoday.com/story/tech/2014/11/03/nsa/18444461/

Survey: Cybersecurity priorities shift to insider threats
http://www.federaltimes.com/article/20141103/FEDIT03/311030016/Survey-Cybersecurity-priorities-shift-insider-threats

Washington Debrief: Senate Leaders Say Cybersecurity Legislation Must Pass This Year
http://www.healthcare-informatics.com/article/washington-debrief-senate-leaders-say-cybersecurity-legislation-must-pass-year

Extracting data from air-gapped computers via mobile phones
http://net-security.org/secworld.php?id=17583

8 Tips on Cyberthreat Information Sharing
http://www.govinfosecurity.com/8-tips-on-cyberthreat-information-sharing-a-7520

New Apple-focused malware uses Macs to infect iPhones
http://www.cnet.com/news/new-apple-focused-malware-uses-macs-to-infect-iphones/

New 'WireLurker' malware targets Chinese Apple users, hops from OS X to iOS via USB
http://appleinsider.com/articles/14/11/05/new-wirelurker-malware-targets-chinese-mac-and-ios-device-owners

Cybersecurity's All-Seeing Eye
http://www.businessweek.com/articles/2014-11-06/cybersecurity-software-companies-seek-integrated-solution

Former NSA lawyer: the cyberwar is between tech firms and the US government
http://www.theguardian.com/technology/2014/nov/04/nsa-cyberwar-stewart-baker-cloudflare-snowden

Cybersecurity 2014: Breaches and costs rise, confidence and budgets are low
http://www.csoonline.com/article/2843820/data-protection/cybersecurity-2014-breaches-and-costs-rise-confidence-and-budgets-are-low.html

What attackers do after bypassing perimeter defenses
http://net-security.org/secworld.php?id=17595

Impact of GOP Win on Cyber Lawmaking
http://www.govinfosecurity.com/blogs/impact-gop-win-on-cyber-lawmaking-p-1770

NSA Director Says Agency Shares Vast Majority of Bugs it Finds
http://threatpost.com/nsa-director-says-agency-shares-vast-majority-of-bugs-it-finds/109170

Cyber bill advocates pin hopes on GOP Congress
http://thehill.com/policy/cybersecurity/223442-cyber-bill-advocates-pin-hopes-on-gop-congress

Cyber crime targets feds
http://www.martinsvillebulletin.com/article.cfm?ID=44194

Fileless malware runs entirely from memory to make detection harder
http://betanews.com/2014/11/10/fileless-malware-runs-entirely-from-memory-to-make-detection-harder/

Cybercrime Gang Targets Execs Using Hotel Internet
http://blogs.wsj.com/digits/2014/11/10/cybercrime-gang-targets-execs-using-hotel-internet/

Massive Takedown Shutters Cyber-Crime Services on Tor Network
http://www.eweek.com/security/massive-takedown-shutters-cyber-crime-services-on-tor-network.html

How to Avoid the 'Biggest' iPhone Malware App Attack Yet
http://time.com/3560875/iphone-malware-wirelurker/

Silk Road, other Tor "darknet" sites may have been "decloaked" through DDoS
http://arstechnica.com/security/2014/11/silk-road-other-tor-darknet-sites-may-have-been-decloaked-through-ddos/

Keeping cybersecurity focused on critical infrastructure
http://www.euractiv.com/sections/infosociety/keeping-cybersecurity-focused-critical-infrastructure-309893

Big Data: Cyber Security's Silver Bullet? Intel Makes the Case
http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/

Home Depot, Target: Same Breach Script?
http://www.govinfosecurity.com/home-depot-target-same-breach-script-a-7544

Hacker Wars: Companies Fight Back With Counter-Intelligence
http://www.nbcnews.com/news/us-news/hacker-wars-companies-fight-back-counter-intelligence-n243936

BlackEnergy malware threat has some cybersecurity experts uneasy
http://www.securityinfowatch.com/news/11769414/cybersecurity-experts-uneasy-about-threat-posed-by-blackenergy-malware

U.S. fights cybercrime from suburban office parks
http://www.securityinfowatch.com/news/11769351/us-cybersecurity-centers-hide-in-plain-sight

POS Malware Continues To Evolve
http://www.darkreading.com/attacks-breaches/pos-malware-continues-to-evolve/d/d-id/1317408

Under Attack: Your Bank, Your Grid, Yourself
http://www.bloombergview.com/articles/2014-11-13/under-attack-your-bank-your-grid-yourself

Five Cyber Security Takeaways From the Mid-Term elections
http://www.huffingtonpost.com/brian-e-finch/five-cyber-security-takea_b_6141914.html

US, China see little progress on cybersecurity
http://thehill.com/policy/cybersecurity/223865-us-china-see-little-progress-on-cybersecurity

University of Maryland hosts girls' cybersecurity career workshop
http://www.diamondbackonline.com/news/article_04d5a9a0-6aea-11e4-b9f3-1bbb47a920b7.html

Let the right one in: Apple uses two doors to manage malware
http://www.macworld.com/article/2847465/let-the-right-one-in-apple-uses-two-doors-to-manage-malware.html

Evidence implicates government-backed hackers in Tor malware attacks
http://www.theguardian.com/technology/2014/nov/14/government-hackers-tor-malware-attacks-onionduke-miniduke

How a Russian Dark Web Drug Market Outlived the Silk Road (And Silk Road 2)
http://www.wired.com/2014/11/oldest-drug-market-is-russian/

The future of war: Cyber is expanding the Clausewitzian spectrum of conflict
http://ricks.foreignpolicy.com/posts/2014/11/13/the_future_of_war_cyber_is_expanding_the_clausewitzian_spectrum_of_conflict

RI Dem: Cybersecurity education should be top priority
http://thehill.com/policy/cybersecurity/224052-ri-dem-cybersecurity-education-should-be-top-priority

8-Year-Old Indian-Origin CEO to Give Lecture at Cyber Security Summit
http://www.ndtv.com/article/india/8-year-old-indian-origin-ceo-to-give-lecture-at-cyber-security-summit-620044

Best practices for government agencies to secure IT infrastructure
http://net-security.org/secworld.php?id=17636

Retail Trade Groups Want Fair Data Breach Reporting Rules
http://threatpost.com/retail-trade-groups-want-fair-data-breach-reporting-rules/109305

Carmakers promise they'll protect driver privacy -- really
http://www.computerworld.com/article/2847403/carmakers-promise-theyll-protect-driver-privacy-really.html

US State Department targeted by hackers
http://net-security.org/secworld.php?id=17646

Scotland Yard wages war on 200 cyber crime gangs in London
http://www.standard.co.uk/news/crime/scotland-yard-wages-war-on-200-cyber-crime-gangs-in-london-9864993.html

Authorities nab WireLurker masterminds
http://www.scmagazine.com/authorities-nab-wirelurker-masterminds/article/383567/

U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies

http://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/

Facebook, Google and Apple lobby for curb to NSA surveillance
http://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance

Cyber bill's fate hinges on NSA reform
http://thehill.com/policy/cybersecurity/224281-cyber-bills-fate-hinges-on-nsa-reform

Privacy is the new killer app
http://www.computerworld.com/article/2846446/privacy-is-the-new-killer-app.html

Majority of Firms Would Hire Ex-Cons as Cyber-Security Pros
http://www.infosecurity-magazine.com/news/firms-would-hire-excons-as/

Microsoft Considering Public-Key Pinning for Internet Explorer
http://threatpost.com/microsoft-considering-public-key-pinning-for-internet-explorer/109365

State Department Shutters E-mail System
http://www.govinfosecurity.com/state-department-shutters-e-mail-system-a-7565

Civil liberties groups vow to fight on after Senate kills NSA reform bill
http://www.theguardian.com/us-news/2014/nov/19/senate-kills-nsa-reform-bill-civil-liberties-groups

Cyber war games held
http://www.washingtontimes.com/news/2014/nov/12/inside-the-ring-cyber-war-games-held/

Hacker Lexicon: What Is the Dark Web?
http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

New House Intel chief viewed NSA reform as unnecessary
http://thehill.com/policy/technology/224627-new-house-intel-chief-viewed-nsa-reform-as-unnecessary

WhatsApp Adds Encryption by Default to Android App
http://threatpost.com/whatsapp-adds-encryption-by-default-to-android-app/109442

DDoS attacks continue to fall in size and frequency
http://net-security.org/secworld.php?id=17657

10 hottest IT skills for 2015
http://www.computerworld.com/article/2844020/careers/10-hottest-it-skills-for-2015.html

IG: DHS Struggles to Manage Privacy
http://www.govinfosecurity.com/ig-dhs-struggles-to-manage-privacy-a-7574

Unscheduled Windows update kills critical security bug under active attack
http://arstechnica.com/security/2014/11/unscheduled-windows-update-kills-critical-security-bug-under-active-attack/

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

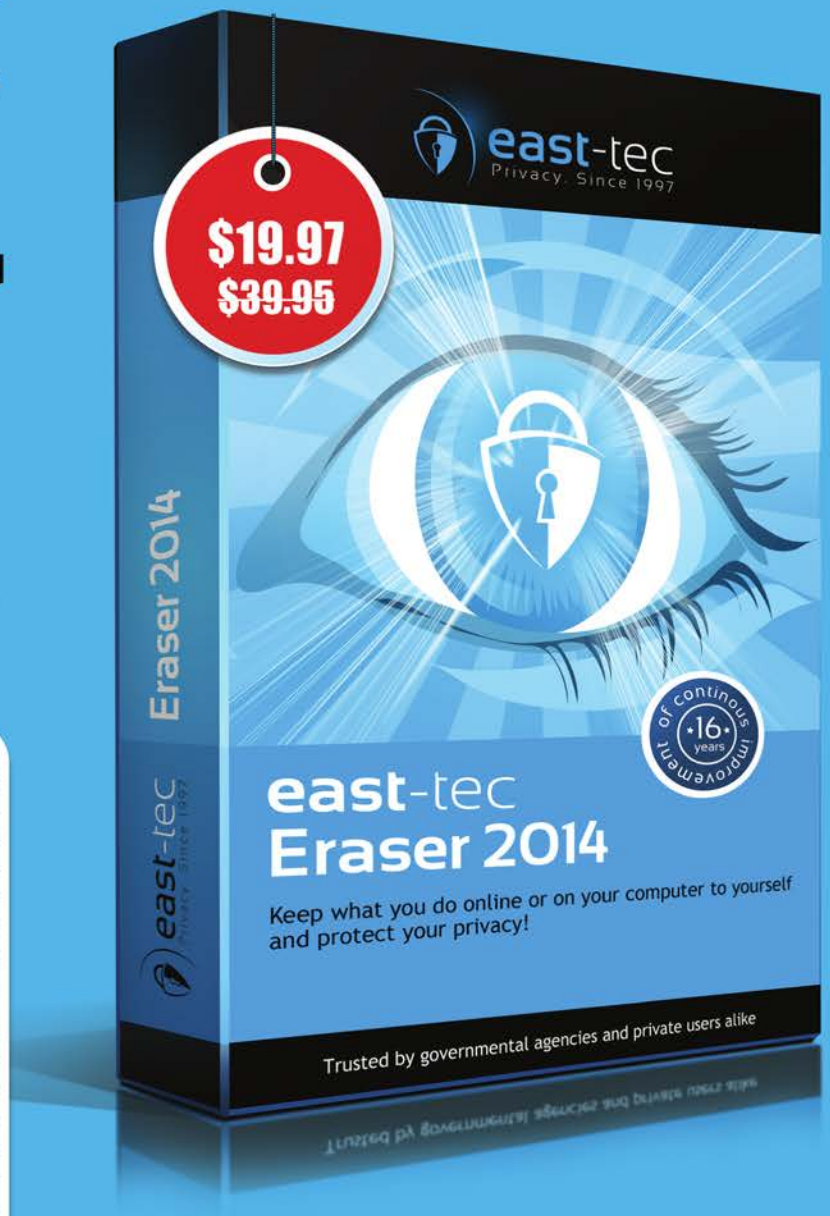
Cyber Defense Magazine - Cyber Warnings rev. date: 11/21/2014

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

Protect your data and privacy by removing all evidence of your online and offline activity with **East**-Tec **Eraser 2014**.
Securely erase your Internet and computer activities and traces, improve your PC performance, keep it clean and secure!



Exclusive offer for Cyber Defense magazine readers

Save 50%

on ALL East-Tec products
www.east-tec.com

Coupon Code:

CYBERMAG2014

private evidence protection traces from 250 + apps history pages online privacy secure search pictures cookies security emails