CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Compliance
Technology Automation
Advanced Threats
Information Governance

June 2015

MORE INSIDE!

CONTENTS

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

Lee Ying
Robert B. Dix, Jr.
Alan McQuinn
Alina Stancu
Todd Weller
Luis Corrons
Matt Zanderigo
Tim Liu
Milica Djekic
Jeremy Stieglitz
Daniel Nieten
Max Nomad
Mav Turner

Interested in writing for us:
marketing@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®

2015 Malware RATs and Cybercrime is Out of Control

Friends,

You can't open your eyes in the morning without reading about another breach. As you know, I like to cover the most breaking cybercrime and cyber threat news each day at Cyber Defense Magazine. I don't have to look far for hackers to be breaking into an Airline or a Bank or showing how weak and insecure critical infrastructure is, to simple attacks going after common vulnerabilities.

Then we look to the east and we find some of the most advanced zero-day malware and remote access Trojans being developed on a daily basis by the Chinese. Some is for the government but it also seems that some is for profit. As Brian Krebs points out in his weekly blog, there's much for sale on the black market. One breach and a million records makes you a millionaire. Sure, you'll be running from the law but maybe not in the deep dark alleyways of a Chinese Hutong. You might even be working for the Chinese government by day – helping perform cyberespionage for your government as your paid job but act, unfettered, as a cyber-criminal by night. If they need to hack into a mail server for spear phishing reconnaissance, they do it, as you can see here at http://map.ipviking.com

This quiet cyber war and ongoing cyber crime has sparked some of the biggest breaches and reactions in history – from the Sony Pictures breach by what appears to be the North Korean government (DPRK) to the recent Anthem breach (over 80,000,000 'fullz' records – all the PII anyone would want on 1/4th of the entire American population), we're looking at these events becoming astronomical in data theft, damages and costs.

Meanwhile, what you don't read about in the news are all the SMBs (Smaller to Medium Sized) businesses getting attacked. In fact, when one SMB is exploited, there's a 50% chance they will go out of business. It's simply that costly for them to recover from a full network breach or PII data theft. In America, over 80% of the companies are SMBs, so yes, they are also a rich target for many of the hackers who don't want to be the cover story on the newspaper or mainstream media. The biggest thing that Sony Pictures, Anthem and SMBs all have in common is one thing – people getting infected with RATs. As you read no through this month's edition of Cyber Warnings, think about your organizational goals. Have you included training against Spear Phishing, Social Engineering and RAT infections as a top priority? If you haven't, now is the time.

To our faithful readers, Enjoy

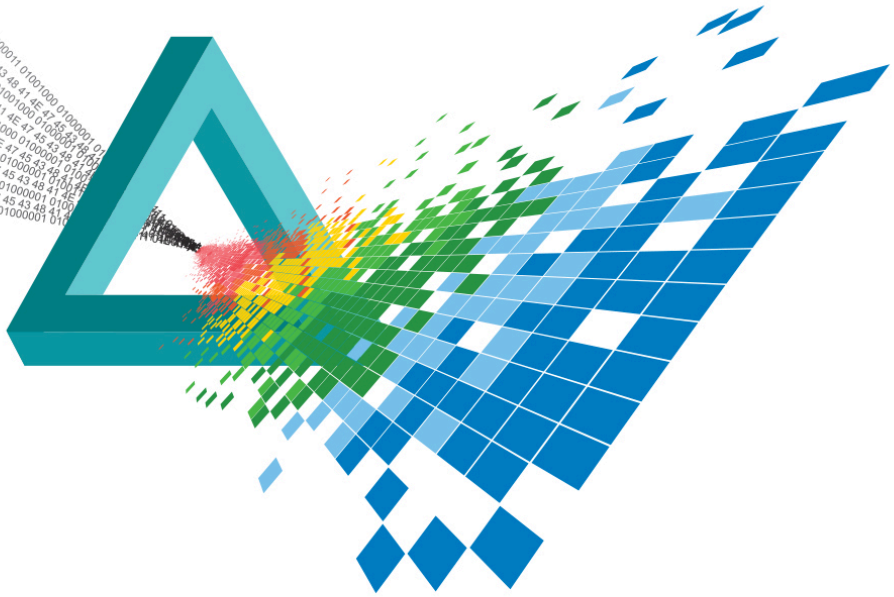
Pierluigi Paganini

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

RSA Conference2015

Singapore | 22-24 July | Marina Bay Sands

Save S$150 on your Full Conference Pass
during the Early Bird period
Early Bird ends June 20



CHANGE

Challenge today's security thinking

Register now for RSA® Conference Asia Pacific & Japan 2015

The theme for this year—CHANGE—is a timely reminder of the importance of challenging today's security thinking. Attend RSA Conference Asia Pacific & Japan to keep up with the changing dynamics of cyber security.

- **7 tracks**
- **60+ Sessions**
- **100+ Exhibitors**

Experience these exciting programs:

- **RSAC Innovation Sandbox Most Innovative Start Up**
- Great lineup of **Keynote speakers**

Guest Keynote Speaker
AMIT YORAN
President, RSA

FOLLOW US ON: #RSAC

Register Now! www.rsaconference.com/CDM

Supported by: SINGAPORE EXHIBITION & CONVENTION BUREAU

Managed by: Singex

Held in: YourSingapore

3 World Famous Computer Viruses and What We Can Learn From Them

They've caused billions of dollars' worth of damage. They've delayed planes, grounded military helicopters, and brought down ATM networks. Dozens of computer viruses have haunted internet users for decades now, but a few viruses stand out among the rest as having been particularly devastating.

Fortunately, by looking at the lessons learned with each computer virus pandemic, we can enhance our security protocols and look forward to a safer future.

Physical security is relatively an easy task, as technology continues to grow the physical security scene continues to improve.

Gone are the days when a full staff of bodyguards were needed and nowadays a full set of advanced cameras such as the ones pro-vigil provides are all we need.

SQL Slammer Crushed Businesses and Brought the Web to a Crawl Because Nobody Expected It

A virus that focused on web servers, SQL Slammer caused hundreds of millions of dollars in damages within only a few minutes. The virus spread so quickly that its number of hosts doubled every few seconds. It infected nearly half the servers that keep the internet running.

The virus focused on a vulnerability in SQL server software, so most home computers were not affected.

However, the internet slowed to a crawl, and many server dependent organizations suffered devastating outages. Among the worst outages were those experienced by Continental Airlines, Bank of America's ATM service, and Seattle's 911 service.

Part of the problem was that many of the businesses attacked had no contingency plan in place for such an emergency. It isn't enough to simply have powerful security and anti-virus measures, you should also have a plan in case your security measures fail.

MyDoom Threatened to Bring Down Google Because Millions Opened Unknown Attachments

Days after 2004's MyDoom began spreading itself via email, it was declared the fastest spreading computer virus ever. MyDoom started on peer-to-peer file-sharing networks and continued its spread via email. Unlike common computer viruses though, MyDoom didn't simply get new email addresses from a host's account, it also searched Yahoo and Google for additional email addresses.

At its worst, as many as 1 out of every 4 emails sent contained the MyDoom attachment. Once millions of computers were infected, MyDoom's collective billions of web searches per second crushed the response time of the overwhelmed search engines.

Ultimately, the virus could only spread the email attachment itself though, since users had to actually click on the Trojan horse file for their machine to become infected.

That means that every single one of these users opened at least one file without knowing what it was!

The lesson from MyDoom was that people must be better educated on not opening unknown file attachments or downloads. Curiosity can and does kill the cat.

Conficker Preyed on a Publicly Available Windows Flaw and the Sharing of Flash Drives

One particularly persistent and prevalent worm, Conficker, continues to infect computers to this day, but the virus may have fallen prey to its own success. At its height, experts estimate that Conficker had infected as many as 15 million computers. Estimates put the total economic damage of the Conficker worm near $9 billion! This is partially because it rapidly spread through business and government networks in Europe and the Middle East that were in the habit of sharing flash drives, which Conficker exploited in addition to spreading via email. USB sharing poses a significant physical security risk to computer networks.

The worm was built to hijack computers by exploiting a flaw in Windows. Strangely, this flaw was revealed by Microsoft themselves when they released an update to correct it. Unfortunately, many people did not update immediately, and Conficker simply spread faster than the update. This demonstrates how important it is to carefully control information about security risks, and update your systems ASAP.

Fortunately, the worm spread *so* rapidly that cyber-security firms throughout the world detected it very quickly and took it very seriously. A multinational counter-virus task force was created. It succeeded in slowing Conficker's growth and stopped it from communicating with its creator. Whatever devious purpose that person had for the worm, it could never achieve its ultimate goal, possibly preventing the billions of dollars in damages from becoming trillions of dollars. The day was saved due to many companies putting aside their differences and joining forces.

About the Author:

Lee Ying has over 10 years experience in the tech and security industry. He currently writes for various websites, if you would like to contact him you can find him on LinkedIn: https://www.linkedin.com/pub/lee-ying/9a/18b/238. Follow me on Twitter @LeeYing101

Federal Acquisition Practices Are A Key Contributor to Cyber & Supply Chain Risk

A continuing focus on cost rather than authenticity of products and services is an outdated and increasingly risky approach to federal procurement

Presented by: Robert B. Dix, Jr.

At a time when the challenges of cybersecurity and supply chain assurance continue to be topics of great attention nationally and globally, it remains elusive to understand why the US government has not taken the appropriate step to require federal departments and agencies to purchase information and communications technology (ICT) products and services from authorized sources, at least for high impact and mission critical systems.

Instead, the ongoing culture of meeting acquisition cost and schedule parameters by purchasing ICT products and services based on a lowest price, technically acceptable (LPTA) approach is a contributor to the growing cybersecurity risk. The pressure to save acquisition dollars may result in government contracting officials deciding to purchase from untrusted resellers. By purchasing ICT products and services from online brokers and other untrusted sources, the risk of acquiring counterfeit, tainted, or even malicious equipment is significantly increased.

Most Original Equipment Manufacturers (OEMs) have made significant investments to create and implement extensive product assurance and supply chain risk management programs which are comprehensive, from product concept to delivery and disposal. Such programs include measures that afford component traceability and history of the product path, including assembly and delivery. Given the global nature of most supply chains, such programs are necessary to affirm product integrity and authenticity.

Additionally, many (OEMs) have business relationships with partners and resellers that offer their products and services to interested acquirers, including government. In order to be included in the approved channel of partners and resellers, OEMs conduct a vetting process to affirm the veracity of the entity, often including background checks, site visits, financial evaluations; and other criteria to validate the credibility of the business. Contractual elements of the engagement allow for entities to be dismissed from the authorized channel if they fail to sustain the requirements established by the OEM. While there is no absolute solution that eliminates all risk, such a review process can certainly reduce the risk and provides greater assurance of the authenticity of the products and services provided.

However, far too often, the government pursues acquisition practices that are driven solely by cost. To be clear, the men and women who are procurement professionals are pursuing their craft based on the long-standing culture of saving money and meeting delivery schedules. In fact, their own performance evaluation may rely on their success in this area. This culture does not consider product authenticity, security, or assurance, and therefore may drive well meaning folks to shop online, in the gray market, or with other untrusted sources seeking to save dollars on whatever product or service they are looking to acquire on behalf of the end user. Given the

current risk environment, this is a dangerous practice that contributes to cybersecurity and supply chain risk by increasing the possibility of receiving counterfeit, tainted, or even malicious products and services.

In most cases when ICT products and services are not acquired directly from the OEM or from their authorized partner / reseller channel, they are not eligible for warranties or technical support, thus increasing business risk in addition to cyber risk.

Sadly, there are many documented examples of acquisitions that resulted in delivery of equipment that did not properly function; instances where boxes appeared to have been tampered with; and / or trying to determine at delivery if the product in the box is authentic or even new. This presents unnecessary risk to the government, and should be of great concern especially as it regards high impact and mission critical systems.

Many in government look at the private sector as the culprit in the growing cybersecurity and supply chain risk management challenge. However, the opportunity for government to address and implement solutions that will immediately reduce risk by addressing their dated acquisition practices which focus on cost and schedule and do not consider security and authenticity as primary measures of the procurement evaluation process is way past due.

Recently, we have seen language in Request for Information documents (RFI's) and Request for Proposals (RFP's) that actually address this issue and require a prospective provider to attest to the authenticity of the products and services offered, even validating that the acquisition would be from an authorized OEM or one of their designated partners or resellers. Those examples are sporadic and should become required practice in federal procurements.

Some argue that such practices would be cumbersome for acquirers attempting to deal with obsolescence and the need to purchase replacement parts that may no longer be manufactured by the OEM. This is a valid issue, but it too can be addressed. If a department or agency decides to try maintaining and extending the life of a system where original parts are no longer available, then an acquisition to procure such parts should include a Justification and Approval (J & A) in writing and that is signed by an authorized designated approving authority. This would shift any liability from the OEM to the acquirer who chooses to make such an acquisition from the gray market, from an online broker, or some other untrusted source.

We also must remember that our adversaries know about these acquisition practices and they have exploited the government's systems and supply chain by flowing non-secure and non-authentic products into broker and gray market channels used by procurement officials. The often false presumption that the lower advertised pricing from unauthorized providers is saving money and meeting acquisition requirements, can produce potentially debilitating results. In the current risk environment and with a history of evidence illustrating the use of different tactics, techniques, and procedures by criminals and adversaries to penetrate government systems and supply chain through the acquisition process, it is a potentially dangerous approach to continue practices that focus on cost and schedule without sufficient checks and balances to validate authenticity of products and services purchased. Our national and homeland security demand

that we no longer support an acquisition process where we potentially expose significant exploitable risk in this manner.

If ever there was an issue that was ripe for Executive action, this is it. In order to change the culture, it requires no-nonsense leadership and direction. Executive action should be offered immediately that directs federal departments and agencies to only acquire information and communications technology products and services from authorized providers, at the very least for high impact and mission critical systems.

There are ongoing efforts being considered by the US Department of Defense; General Services Administration; Department of Homeland Security; and others to examine this issue. However, those activities have lagged and thus far have not produced any tangible measures to address this significant cybersecurity and supply chain risk challenge. Accordingly, in order to lead by example, the Administration should take immediate steps to direct federal departments and agencies on this matter. The cultural issues have to change from acquisition practices being exclusively about meeting requirements for cost and schedule, to include evaluation criteria that address authenticity, security, and assurance of products and services purchased. This will require leadership and a clearer understanding of the risk, including the business risk.

We all understand the impact of reduced budgets and how they impact decision making around the acquisition process. The old Midas commercial talked about “pay me now or pay me later”. Similarly, in the case of information technology and communications hardware, software, and services, it is imperative that we make every effort through the acquisition process to purchase those products and services from authorized providers. Without specific policy guidance and direction, and with increasingly austere budgets for department and agencies, this challenge could get worse as procurement officials focus even more on saving dollars in the acquisition process.

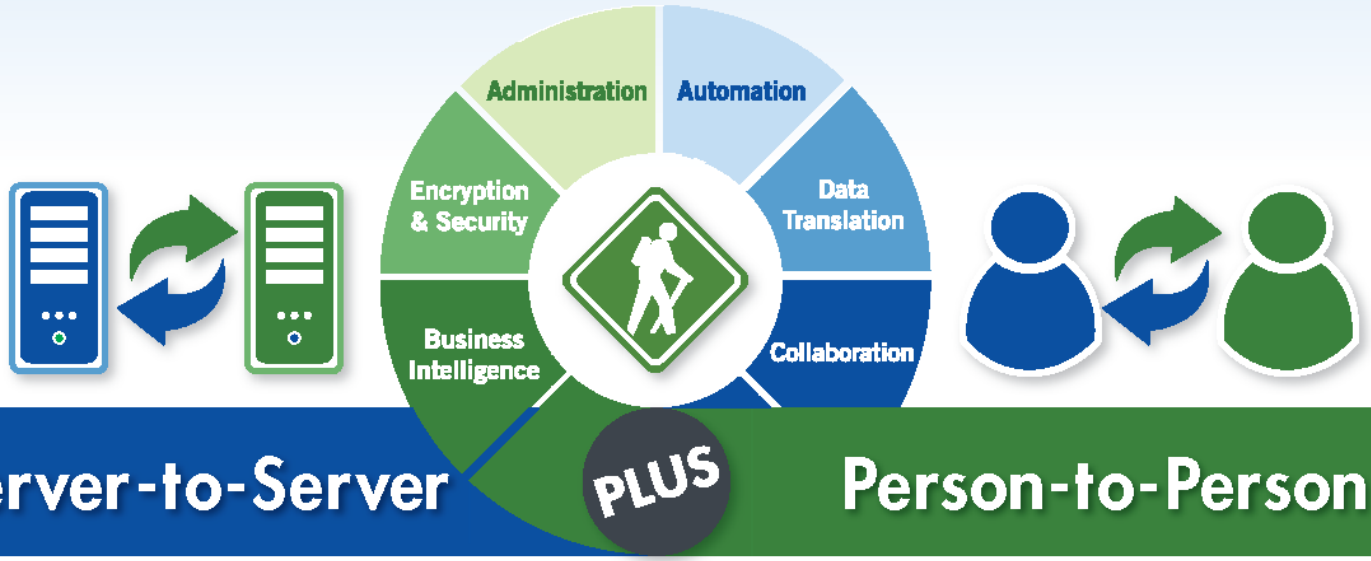
Industry and government working together collaboratively will be able to address this matter in a proactive and productive manner in efforts to drive a policy that updates the federal procurement process to reduce the risk to cybersecurity and supply chain assurance thereby improving national and economic security and resilience.

The risk is real. This time is now. Let’s get to it.

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.

Secure File Transfer



Simplify File Transfers with GoAnywhere™

GoAnywhere Managed File Transfer automates and secures file transfers with your customers, vendors and enterprise servers.

Through a browser interface, GoAnywhere MFT allows your organization to connect to almost any system (internal or external) and securely exchange data using a wide variety of standard protocols.

GoAnywhere MFT can parse XML, CSV and XLS files to/from databases, and includes the ability to encrypt file transfers using Open PGP, SFTP, FTPS, AS2, HTTPS and AES.

Visit GoAnywhere.com for a free trial.

"GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).

We currently have 45,000 scheduled and 'triggered' transfers running daily."

One of the Largest North American Railroads

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

Try it for FREE

Seeking a Balance in U.S. Economic and National Security Interests

By Alan McQuinn

Congress recently passed legislation to curtail several of the National Security Agency's (NSA) surveillance programs, focusing primarily on limiting the agency from directly collecting bulk phone records on U.S. citizens. While this reform was a solid first step in the right direction to protect the civil liberties of U.S. citizens, Congress has not yet addressed the economic concerns raised by pervasive electronic surveillance. That is critically important, because the perception that the U.S. intelligence community engages in widespread electronic surveillance continues to severely undercut the U.S. tech industry's global competitiveness. Foreign customers fear that U.S. companies may be more vulnerable to NSA surveillance than their non-U.S. counterparts. Until U.S. policymakers address these concerns, U.S. companies will continue to face a disadvantage selling their products and services abroad.

The Information Technology and Innovation Foundation (ITIF) released a report two years ago in which it estimated that if U.S. cloud computing providers experienced even a modest drop in their expected foreign market share due to concerns over U.S. surveillance then it could cost the United States between $21.5 billion and $35 billion by 2016. However, since that initial report, it has become clear that the whole U.S. tech sector has suffered as a result of the NSA revelations, not just cloud computing firms. Indeed, the economic impact of U.S. surveillance is likely to far exceed our initial estimate. That is the key finding of a new ITIF report updating the original analysis. The new report catalogues a wide range of examples of economic harm done to U.S. businesses and concludes there is no end in sight to these continued losses. Making matters worse, not only are foreign customers shunning U.S. companies, but foreign governments are also using surveillance fears to create protectionist policies that keep out U.S. businesses.

The economic costs of U.S. surveillance

Foreign customers have started to pass on U.S. technology in favor of foreign alternatives. For example, Cisco saw its sales interrupted in Brazil, China, and Russia because of reports that the NSA had secretly inserted backdoor surveillance tools into its routers, servers and networking equipment. In fact, during a quarterly earnings call, Cisco CEO John Chambers even cited the NSA as the factor behind steep sales decreases, saying "I do think (the NSA revelation) is a factor in China." Similarly, IBM, Microsoft, and Hewlett-Packard also have reported diminished sales in China as a result of U.S. surveillance tactics.

At the same time, foreign companies have made the U.S. digital surveillance policy a focus of their own marketing strategies. German cloud companies have started to bill themselves as "Cloud Services: Made in Germany," while Finish companies like F-Secure make the pitch that they never share their users' data with other governments or companies. This strategy has proved effective and F-Secure saw its user-base grow to over one million within the first nine months of operation.

Foreign governments are also dropping contracts with U.S. firms in favor of foreign providers. For example, the German government dropped Verizon over fears that the NSA used their services as spy tools. In addition, China recently took prominent U.S. tech firms off of its approved purchase lists, ostensibly due to U.S. cyberespionage. Because the Chinese government owns some of the world's largest banks and those organizations can only buy products on these lists, loss of access hurts several U.S. tech companies, including Apple, Cisco, and Intel's McAfee.

Foreign countries claim U.S. surveillance justifies protectionism

Foreign governments are using U.S. surveillance as justification for protectionism. While these countries say they are trying to protect their citizens from the prying eyes of the NSA, it is clear that many of them are focused more on misguided attempts to spur their own economies than by any real efforts to limit surveillance. By creating rules that advantage domestic firms over foreign firms, many countries believe they will build a stronger domestic tech industry. For example, some in Europe have called for preferences for domestic providers and even a system that keeps European data in Europe, called the "Schengen area for data," as means to promote deployment of European-focused cloud services. As a result, Amazon started running Internet services out of Germany for its European business partners in an effort to downplay threats of online spying.

There is also a trend in countries, such as Australia, China, and India, of creating laws that prevent certain data from leaving the country's borders. This effectively requires cloud computing firms to build data centers in those countries or risk giving up market access. For example, in 2014 Russian implemented policies that would require Internet-based companies, such as Google or Facebook, to store personal data of Russian users within the country's borders.

However, these protectionist policies not only limit the number of services that a country's citizens and businesses can enjoy, but also harm that country's productivity and competitiveness. For example, Xero—a cloud-based accounting software company that provides back-end computing to increase the productivity of its customers—has encountered barriers from countries that restrict the flow of data, like China. They also unwittingly hurt the long-term ability of a country's own firms to compete in global markets by sheltering them from international competition.

So how can the United States reverse this trend?

The globally networked economy demands commerce without geographical restrictions. To push back against the trend by some countries to erect geographic borders on the Internet and create a level playing field for the U.S. tech sector, the United States should lead by example and establish the most compelling global standards for transparency, cooperation, and accountability. First, the U.S. government should clearly inform the public about the data it collects domestically and abroad and work with its allies to create similar commitments abroad.

Second, the U.S. government should strengthen its treaties with other nations—called mutual legal assistance treaties (MLATs)—which allow law enforcement agencies to cooperate and

provide assistance to their counterparts in other countries during lawful investigations. While the U.S. government cannot force other governments to stop circumventing this process, it can set an example by reinforcing and abiding by its own and asserting that other countries should do the same

Third, the U.S. government should work to establish international legal standards for government access to data. Just as international aeronautical law was developed to manage the expansion of global civil aviation, so too should countries come together to construct rules governing the global data economy.

Finally, the United States should continue to challenge protectionist policies around the globe by completing trade agreements that prohibit these practices. The United States should build an alliance with the other countries through trade agreements, such as the Transatlantic Trade and Investment Partnership, forcing bad actors to suffer consequences if they continue to enact anti-competitive rules.

Over the last few years, the U.S. government has put intelligence gathering first, allowing the ensuing economic challenge to U.S. tech companies to fester. The cost of U.S. inaction is already too high, impacting economic growth, jobs, and the U.S. trade balance. Indeed, if the U.S. tech sector is to remain competitive, the United States should take decisive steps to balance its economic needs with its national security interests.

See the full report here.

About the Author:

Alan McQuinn is a Research Assistant with the Information Technology and Innovation Foundation. His research areas include a variety of issues related to information technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, Internet governance, and commercial drones. Prior to joining ITIF, he was a telecommunications fellow for Congresswoman Anna Eshoo.

Alan graduated from the University of Texas at Austin with a B.S. in Public Relations and Political Communications, and a Minor in Mandarin Chinese. He spent his final semester at UT as a participant in the Bill Archer Fellowship Program. During his time as an Archer Fellow, he interned for the Federal Communications Commission in the Office of Legislative Affairs.

Can Compliance Gain Customer Trust In Credit Unions?

Financial crime in cyber space is on the rise. The PwC 2014 “Global Economic Crime Survey – Financial Services” analysis shows financial and retail services at greatest risk.

Although the financial industry is a top spender for security and compliance, the figures provided by PwC show that cybercrime accounts for a total of 39% of economic crime.

The 2015 survey announced that the cost of security incidents has jumped 24% with the number of companies that reported losses in the $10m - $20m range increasing by 141%.

For the credit union industry this trend is more than worrying, as credit unions end up with a hefty bill in the aftermath of a credit breach. The Target data breach was estimated to have cost credit unions $5.68 per card affected.

With 40 million card details stolen, the total cost for credit unions came to $227 million. The reality is that financial cybercrime reverberates throughout the supply chain.

So far credit unions have taken a proactive approach in their response to retail breaches. They have been quick to understand that the correct approach in light of a breach is to work alongside the customer and keep them informed of the progress of the fraud.

After the impact of the Target attack, we now see credit unions openly reaching out to their customers and informing them of breaches, while offering advice and resources to check for any signs of fraud.

For example, in the Home Depot breach some credit unions have gone as far as to comb through customer records, looking for any transactions with Home Depot.

However the credit industry is suffering on a different level as well. Specifically, small credit unions appear to be facing a steady decline.

A comprehensive survey carried by the Financial Brand projected a worrying trend for the Credit Union industry; as the big are getting bigger, the small are shrinking to the point where by 2032, one out of every two credit unions will have disappeared.

However, despite the decrease in credit union branch numbers, industry assets are set to go up; proving the public is still showing faith in credit unions.

In the face of such issues, how can the imminent threat of cyber attacks represent a silver lining for credit unions?

The reality is that attacks will continue, and NAFCU has identified small credit unions in particular as vulnerable, as they lack access to extensive IT security budgets and specialist staff. Many small organisations fear finding themselves crippled by regulatory bodies’ increasing measures and standards.

However there are cost effective measures that can be taken, even for the smallest credit unions; a combination of network security auditing, continuous monitoring and mitigation solutions can be the low cost answer to meeting the call for tighter regulations set by NAFCU and it is a great way to show commitment to security.

Furthermore, credit unions that address the issue of information security in this way stand a great chance of turning cybersecurity and compliance into business enablers and use it as a positioning strategy to gain consumer trust, in an industry where confidence is deprecating rapidly.

Companies do not have a choice in stopping cybercrime, but they can choose how they respond to it.

About the Author:

Alina Stancu is the Marketing Coordinator for Titania, a software company that supplies network security audit and compliance software to auditors and enterprises. Alina comes from a non-technical background, but the time spent in the information security industry has placed her at the confluence between cybersecurity, communications and business. Part of her job is striving to make security enter the mainstream discourse for a variety of economic, political or social contexts.

(ISC)²

SECURITY CONGRESS | APAC 2015

Co-organized by

28-29 July 2015

Manila, Philippines

Sofitel Philippine Plaza Manila

Join (ISC)² for 2 days of insightful discourse and hands-on workshops as top-notch InfoSec luminaries representing academia, government and industry from Americas and Asia discuss emerging threats, best practices, and solutions to challenges.

30 International Speakers

2 Days

25 Sessions


Hon. Jejomar C. Binay
MNSA
Philippines


David Shearer
CISSP, PMP
U.S.A.


Sanjay Bahl
CISM, CIPP/IT
India


Darren Cerasi
Singapore


Chuan-Wei Hoo
CISSP, CISA, CFE, BCCE
Singapore


Masaru Horioka
Japan


Dr. Meng-Chow Kang, CISSP
Singapore


Haruto Kitano
CISSP, JGISP
Japan


Dave Lewis
CISSP
Canada


Prof. Howard A. Schmidt
CISSP, CSSLP
U.S.A.


Prof. Corey Schou
CSSLP
U.S.A.


Prof. Jill Slay AM
CISSP, CCFP
Australia


Freddy Tan
CISSP
Singapore


Dr. Wan Suk Yi
CISSP, ISMS
Korea

Attended by **350** Information Security Professionals in 2014

- Keynote Presentations
- Interactive Sessions
- Regional Roundtable Discussion with information security experts
- "Management & Strategy" and "Technical" tracks plus hands-on workshops

3 Hands-on Workshops

- Web Security: Why your CISO doesn't sleep
- DDoS: Barbarians at the Gate(way)
- Forensics

Platinum Sponsor

CYBERARK

Gold Sponsor

hp Enterprise Security

Silver Sponsor

QUALYS® CONTINUOUS SECURITY

REGISTER NOW

Special Price - USD 306 (Discount code: MCDM)

Standard Pass - USD 340

For Inquiries:
(852) 2850 6953
securitycongressapac@isc2.org

Visit **apaccongress.isc2.org**

Analytics + Integration + Automation = Improved Security Response

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

A recent article by Kenneth Corbin reviews the findings of a study from Meritalk and sponsored by Splunk, and discusses how government security workers are struggling with Big Data and that better analytics could improve their security posture.

The article also indicates tight security budgets are a major challenge.

As far as the conclusions, I'm not surprised. The Big Data security alert overload problem is a challenge for both government and commercial organizations, and with trends like mobile and Internet of Things, this will only worsen.

Budget pressures are also endemic to all organizations though some worse than others.

Improved Security Analytics One Piece of the Puzzle

Improved security analytics are clearly needed. Hexis, along with other vendors like FireEye, Palo Alto, and Splunk, are working to address this.

For example, with our recent launch of HawkEye G 3.0 we unveiled our ThreatSync™ capability, which fuses together our signature-less endpoint detection and network detection with 3rd party indicators from FireEye and Palo Alto Networks. These indicators are combined into a unified scoring model.

We believe that corroboration and analytics will result in reduced alert overload and improve the signal-to-noise ratio. Not coincidentally, we are also integrating with Splunk to improve threat intelligence.

Analytics Should Be Complemented By Automated Threat Removal Capabilities

While improved security analytics are critical to improving security posture, it is just one key component.

In fact, Adam Cohn, director of public policy and government affairs at Splunk, commented that the big data analytics "approach is only one element of the "multi-faceted" framework that government agencies should adopt when evaluating their security posture."

Again, while this article and comment applies to government agencies, I believe it applies to the commercial sector as well.

A Few Automation Use Cases Where You Can Achieve Early Wins

We see a few use cases where customers can begin to experiment with automation and achieve some early wins:

- **Verification of Network Alerts:** Over the last 18 months, many organizations have deployed network-based sandboxes to gain visibility (detect) "advanced threats." While these solutions do provide improved visibility, this is often accompanied by alert overload.

  Additionally, just because a network-based sandbox detects something, it does not mean that an organization is infected. In this case, organizations can leverage automation (machine-guided and/or fully automated) to verify whether endpoints are infected and take the appropriate response. The benefit to organizations is improved efficiency (reduces chasing of "ghost alerts") and an improved security posture.

- **Automated Removal of Nuisance Malware:** In customer deployments over the past 12 months, we have seen that despite deploying numerous security controls, organizations still spend significant time and resources dealing with high volumes of nuisance malware. In this area, organizations can leverage automation to remove these threats serves. The primary benefit here is freeing up your scarce security resources to spend time on more meaningful alerts/threats.

A recent blogpost by Chris Young, General Manager of Intel's Security Group, validated the opportunity to leverage automation to deal with the nuisance malware stating:

"We all can agree that in the landscape we operate in, not all threats are created equal. That's why we need to give ourselves permission to stop going after every alert that comes into our Security Operation Centers with equal focus. Around 98 percent of these events are low priority – let's trust automation to handle them. Instead, we should put our talent on the hunt after the two percent of alerts that are the real problem."

Automation Requires Integration

The ability to automate threat removal and response inherently requires orchestration which requires integration. Integration needs to occur both within security solution providers' own product portfolios and also between disparate security providers' solutions.

Despite a revival of the security platform movement from next generation vendors like FireEye and Palo Alto Networks, I expect many organizations will continue to operate with a best-of-breed mentality, deploying multiple security solutions.

At the same time, I do expect organizations to look to consolidation to reduce security sprawl and the associated costs both direct and indirect (i.e. management).

The outcome of these dynamics is becoming increasingly clear: Customers are pushing vendors harder to improve integrations.

Improved integrations not only enable customers to leverage capabilities like automated response, but equally importantly it enables them to get more value out of their existing investments.

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

Immerse yourself in mobile.

To capture a piece of the $1 trillion mobile market, you can't just dip in your toe.
Dive in head-first at CTIA Super Mobility 2015.

Here you'll find every sector of the mobile industry represented by rule-breaking minds and paradigm-shifting technologies that are changing the way we live, work and play.

So, whether you're on the lookout for the products consumers want right now, or the new technology for tomorrow's biggest breakthrough, remember: There's one place where being in over your head is a beautiful thing.

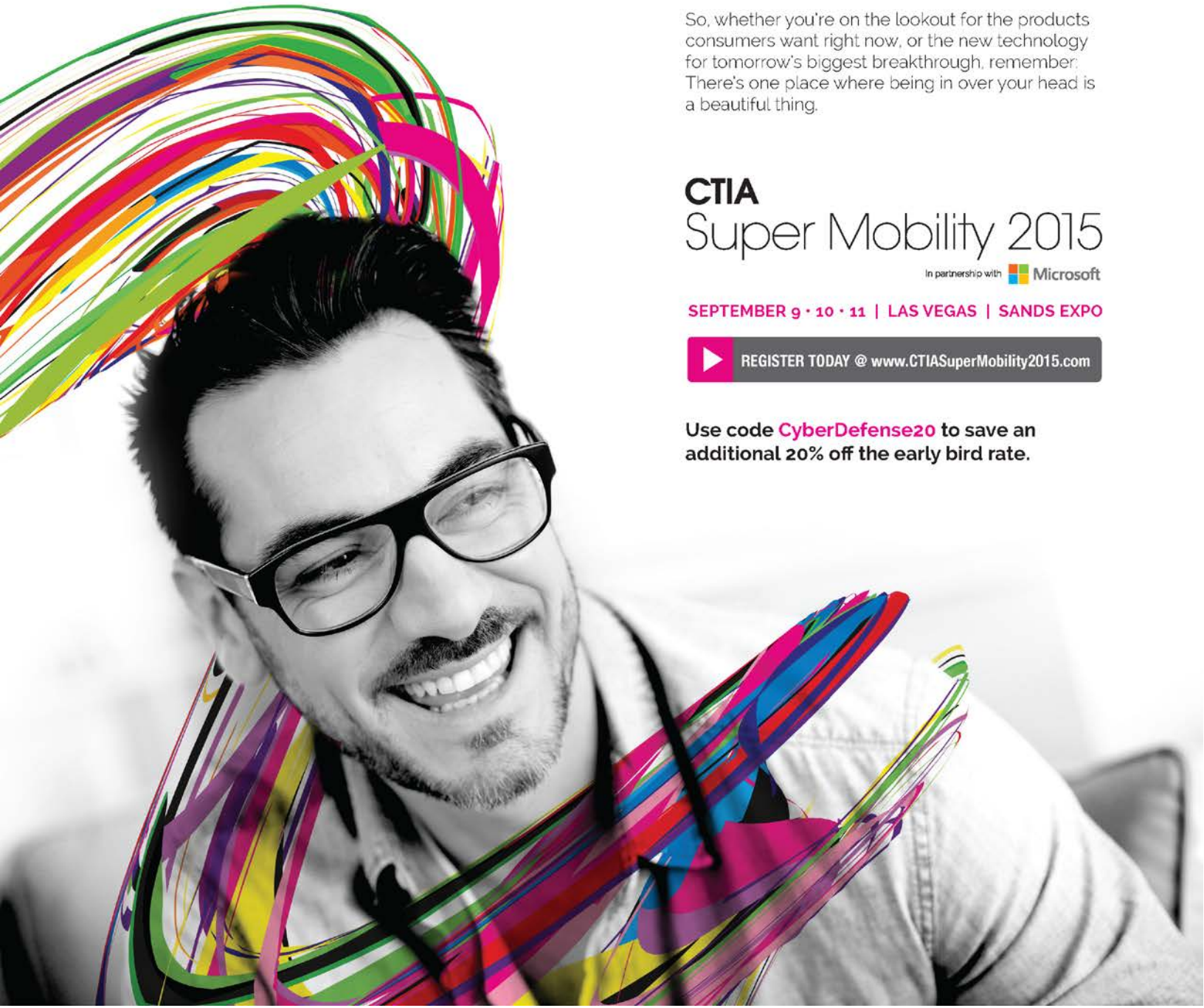
CTIA
Super Mobility 2015

In partnership with Microsoft

SEPTEMBER 9 • 10 • 11 | LAS VEGAS | SANDS EXPO

REGISTER TODAY @ www.CTIASuperMobility2015.com

Use code CyberDefense20 to save an additional 20% off the early bird rate.



Operation Oil Tanker: The Phantom Menace – Cyber Defense Magazine

When you think of the term, 'Phantom Menace', you may think of Star Wars. But to us, as security experts, Phantom Menace represents one of the most sophisticated and malicious cyber-attacks our PandaLabs has ever encountered. It was an attack on the oil industry that its victims are still trying to recover from.

Today, most computer threats are designed to steal information from targeted systems. We examine thousands of cases at PandaLabs because, after all, there are more than 250,000 new malware files are put in circulation every day. The Phantom Menace, however, had gone completely undetected, as it didn't use any kind of malware. It sailed freely under the radar of antivirus engines for multiple companies for years on end.

How did it manage that? The attack was sent using spear phishing, with an attachment called "Document" that used a PDF icon and the file extension ".exe". When we first studied the attack and saw how it was stealing credentials and relaying them to its source, we assumed some kind of Trojan was in play – like Zeus, Netbus, or any of the major Trojan families, which are frequently modified to perform this kind of attack. The "Document" file, though, was a self-extracting file that created a folder, dropped 6 files in and ran one, which was a simple script. The file would then go about opening a real PDF, unzipping a file and executing another script. During this process, credentials were extracted and relayed to the source through the use of legal password recovery tools from browsers and email clients and a simple FTP command from the Operating System.

Since its behavior could not be immediately defined as malicious, it was allowed to work unnoticed by behavior-based detectors. The attack managed to steal credentials from 10 different companies, most of them European, whose main activity was the maritime transport of oil and gas.

Our investigation tracked the source of the Phantom Menace back to Ikeja, a suburb in Lagos, the capital city of Nigeria. Furthermore, we were able to identify a Nigerian citizen who is most likely the mastermind behind this attack.

The next step was clear: inform the authorities so that they could start an investigation and apprehend the person responsible for the hack. For example, one the affected companies was from Spain, leading us to the Spanish Civil Guard – a police force that we have collaborated with in the past and which has a very good reputation in the fight against cyber-crime. Unfortunately, they and other authorities now face a perplexing and challenging problem: to start an investigation, they need a victim who will report the crime. And yet, **none of the 10 known victims of this attack are willing to report it**.

But why? If our theory is correct, the information stolen from these companies has not been used against them, necessarily, but instead to defraud oil buyers. Rather than face the spotlight, they prefer to keep a low profile, change their credentials and continue to operate as though nothing has happened.

Some countries have laws that force companies to report every hacking intrusion where information is stolen. However, that obligation is usually limited to incidents in which the stolen information belongs to a third party (customers, partners, etc.). In this case, the stolen credentials belonged to the company under attack, thereby removing it from obligation to the law to report the theft.

We believe it's time for the next stage: The Force Awakens. Our homage to Star Wars began with the identification of the attack, but now it brings us to the next critical element in the defeat of such a nefarious form of cyber-crime. We are urging all major companies to awaken to their vulnerability, realize that absolute security doesn't exist, and accept that behavior-based protection is limited. It is our hope that they will take steps beyond their standard measures and perform regular audits that can assess and address potential weaknesses in their network security.

Attacks will continue to evolve, and become all the more threatening. Thus, it is the responsibility of companies and security firms alike to continually adapt their defense systems and implement new protection strategies that give total control and visibility over their networks. The Phantom Menace was merely the first of a new kind of attack. Let's be ready for the next.

About the Author:

Luis Corrons has been working in the security industry for more than 16 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.

The Security Threat Trifecta: People, Activity and Applications

by Matt Zanderigo*, Product Marketing Manager,* ObserveIT

Whoever coined the term that "bad things come in three's" probably didn't have security breaches in mind, but it holds true nonetheless. In regards to data breaches and any type of security threat, those three things can be narrowed down to people, activities, and applications.

Threat of People

Users can be targeted by attacks, make mistakes, or even turn malicious, which makes them the weakest link in the security chain. The first step in addressing this risk is to understand the various types of users within your organization and their risk profiles.

Organizations should consider three different categories of people: contractors, IT users, and everyday business users.

Many of the high-profile breaches of the past year (think Home Depot, Target, etc.) were due to contractors' login credentials being stolen. The crippling cyber-attack at Sony has been traced to the stolen credentials of a systems administrator.

Most recently, a 30-year-old rookie financial adviser (business user) at Morgan Stanley stole data on the bank's wealthiest clients. These are just a few examples of each type of user category that has been part of a recent breach.

Threat of Activity

Top activities that put your organization at risk: usage of personal cloud applications, uneducated responses to phishing, configuration changes, and remote access. Employees are opening the door for hackers to enter company infrastructure without knowing it.

Something as simple and unintentional as using personal cloud applications (email, file sharing, screen capturing) for productivity purposes or clicking a link in a phishing email can grant outsiders access to your secure network.

Once inside the network, hackers can perform activities to get complete access to the information for which they are looking (Sudo, account creation and permission changes).

It is extremely difficult to identify unauthorized activity with varying permission levels and the number of admin-related tasks performed on a daily basis (remote access to new systems or leap frogging to different machines).

When organizations fail to notice abnormal activity in context of user categories and other actions, it gives hackers and malicious users time to get valuable data or do real damage.

Threat of Applications

The large majority of users' access data through everyday applications, such as wealth management or portfolio management, to do their jobs, but their actions are hidden in the large volume of data generated through normal user activities.

Companies across a variety of industries rely on business applications that can access their data, such as call center applications, financial systems, EMR/EHR, POS, eCommerce, Billing, Claims processing, portfolio management, CRM, Patient administration, but these applications aren't as monitored or secured as their data storage infrastructures.

Once users login to these critical applications, many organizations have no idea what they are doing. This is making everyday enterprise applications the weak link in today's computer networks.

Each of these toxic combinations of people, activities and applications has one thing in common; they introduce substantial unaddressed user-based risk.

Security-conscious organizations must monitor user accounts to reduce the impact of this type of user-based risk.

Regardless of your monitoring needs, user activity monitoring significantly enhances your security program and allows security teams to mitigate user-based risks in a manner that preserves user privacy.

About The Author:

Matt Zanderigo, Product Marketing Manager, ObserveIT

Matt is currently the Product Marketing Manager for ObserveIT's User Activity Monitoring solution. In this role, he leads the product marketing efforts, solution messaging and the company's freemium strategy.

Matt can be reached online at mailto:Matt.Zanderigo@ObserveIT.com, TWITTER: @MattZanderigo, www.linkedin.com/in/mattzanderigo, and at our company website http://www.observeit.com/

THE CYBER SECURITY SHOW 2015

PROTECT. DETECT. RESPOND.

22-23 SEPTEMBER 2015

SUNTEC SINGAPORE CONVENTION & EXHIBITION CENTRE

CYBER SECURITY STRATEGY FOR IT AND BUSINESS LEADERS

CONFIRMED SPEAKERS

Pierre Noel
CISO, Asia
Microsoft Corporation

Geoff Leeming
Director, Security Engineering & Technology Risk
RBS

Ashish Chandra Mishra
CISO
Tesco HSC

Chin Kiat Chim
Head of Cyber Security
DHL

Vikalp Nagori
Information Security Officer
Citibank

Allan Cabanlong
Chief, Web Services and Cyber Security Division
Philippine National Police

Imran Rahim
Regional Information Protection & Security Officer, APAC
Boehringer Ingelheim

Christophe Durand
Head of Cyber Security
Interpol

Murari Kalyanaramani
Head of Information
Standard Chartered Bank

Sabyasahi Chakrabarty
CSO, Asia Pacific
BT Group

Lim Shih Hsien
Head, Information Security
The Hong Kong Jockey Club

Uday Deshpande
CISO
Tata Motors

Readers of **Cyber Defense Magazine** get an additional 15% off prevailing prices. Quote **XBHS** when booking. Book online at **www.terrapinn.com/cybersecurityasia**

GOLD SPONSOR

Entrust Datacard

SILVER SPONSOR

THALES

MEDIA PARTNER: CDM CYBER DEFENSE MAGAZINE

Continuous Monitoring – New Trend in Spotting Advanced Threats and Insider Theft

by Tim Liu, Chief Technology Officer, Hillstone Networks

Every week, yet another company or agency seems to make the news for having data stolen, either by external attackers or internal thieves. While malware defenses have dramatically improved in recent years and are good at stopping most amateur or broad-based attacks, modern advanced threats now are written by software professionals who have become adept at finding targeted ways into even well-guarded networks.

The picture gets even more complicated with the rise of internal threats. In an era of BYOD, well-meaning employees can inadvertently introduce malicious code into the core of the network, bypassing perimeter defenses.

Add in disgruntled personnel who actively choose to subvert security controls and it's no wonder the old "castle" paradigm of waiting for malicious code to show up, checking its appearance, and then blocking it at the walls if it looks bad is evolving into a more pervasive and proactive approach.

At this year's Gartner Security & Risk Management Summit in early June, Neil MacDonald, VP and Distinguished Analyst at Gartner, described an emerging trend and best practice for network security. He advocates that complete protection requires not just blocking and prevention, but detection and response as well.

To accomplish this, MacDonald recommends a new, more dynamic approach to security that has Continuous Monitoring and Analytics at its core.

In this model, security systems continuously monitor what is happening within networks, applications, and even end-user devices. This goes beyond the historic practice of feeding event logs into SEIM databases and then assembling logic around whatever data happens to be available.

Rather, it puts more intelligence directly into the security systems themselves so that they can keep and process state information locally and apply big-data analytics to identify trends and anomalies.

Unlike simple threshold comparisons, this approach can ferret out information that might not otherwise be available in order to drive more-accurate insights and actions – what MacDonald calls "Context-Aware Intelligence."

This isn't just theory; a variety of security vendors are now using advanced behavioral analysis on data gathered from desktops, servers and networks to look for anomalies in user and application actions.

For example, this approach is now being used in new enterprise firewalls to more effectively keep "bad stuff" out and "good stuff" in. Machine learning techniques dynamically build and

refine a baseline of what is “normal” for different applications and users. Then, traffic is examined in real time using behavioral analysis to recognize previously unknown advanced threats and to identify abnormal actions.

Techniques like behavioral analysis have become increasingly important in the fight against advanced threats because modern, professionally written malware often uses a combination of methods to evade detection by traditional, signature-based scanners.

In particular, code-morphing is widely used by thieves to ensure that no two samples of a given piece of malware look the same.

However, many of these differences are just cosmetic. Verizon found in its 2015 Data Breach Investigation Report that 70% of attacks come from variants of just 20 families of malware. While most attacks look different on the surface, underneath many behave in similar ways.

These similarities make it possible to identify threats that have never been seen before. Statistical analysis of malware samples from around the world has shown that many families of malware exhibit patterns of behavior that can be identified quickly and represented compactly.

New network security devices match these patterns against network traffic in real time to discover potential threats even if the particular form they are taking has never been seen before.

In addition to watching for potentially malicious code that should be blocked, such network security devices also examine the behaviors of traffic associated with users and applications on that network.

These systems typically examine a wide variety of Layer 3 through Layer 7 parameters, ranging from connections per second and bandwidth to URL formation and POST/PUT ratios within HTTP traffic.

This makes it possible to detect not only patently obvious unusual activity such as denial of service attacks and scanning, but also less obvious transfers of data at strange times that might be indicators of compromise or theft (whether by malicious programming or people).

In perimeter deployments, these two types of continuous monitoring complement each other: keeping watch for threats coming in as well as for sensitive data leaking out. However, they also are playing an increasing role internally as organizations cope with the growing number of ways that employees are transferring information into and out of the network.

Rather than assuming the company network is “clean,” many organizations are starting to aggressively segment their network, putting security-monitoring devices throughout.

This way, they can watch for activities that might be particularly unusual for different departments, such as late night transfers from inside Finance or intermittent probes of Engineering systems.

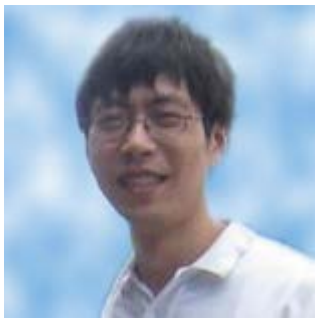
This “behavioral intelligence” enables the devices themselves to be proactive in identifying risks.

Unlike older, static approaches that require manual configuration of fixed sets of parameters to look for, automated continuous monitoring enables risks to be better understood and threats to be prioritized and mitigated more rapidly (in some cases, even automatically).

Ultimately, continuous monitoring provides visibility across the cyber kill chain, giving network security staff immediate insights into attempts at reconnaissance, breaching and exfiltration.

This has become a best practice because it focuses directly on the actions that such code takes, while freeing network security teams from repetitively chasing log files or being inundated with alerts so that they can focus on the bigger picture and more effectively stop attacks.

About The Author:



Dr. Tim Liu is the CTO of Hillstone Networks where he is in charge of product strategies and direction, technology innovation and advanced research. Before joining Hillstone Networks, Mr. Liu was a senior R&D manager in Juniper Networks and was in charge of designing and developing NetScreen's VPN product. Previously, he held positions in R&D and management at Intel, Silvan Networks, Enfashion and Convex Computer, and led technology teams achieving many technical patents. Mr. Liu graduated from the University of Science and Technology in China and obtained a Ph.D. in physics from University of Texas at Austin in 1993.

Tim can be reached online timliu@hillstonenet.com and at our company website http://www.hillstonenet.com/

Register Early and Save!

Cyber Security for National Defense Symposium

Alexandria, VA | August 4-5, 2015 | Mary Gates Center




Featured Speakers Include:

Maj Gen Ed Wilson, Commander, Air Forces Cyber

ADM Mike Rogers, Commander US Cyber Command

Stan Sims, Director, Defense Security Service

New for 2015:

- Strategic initiatives from senior leadership to achieve the 'DoD Cyber Strategy'
- Efforts to increase the capacity and capabilities of National Mission Teams, Cyber Protection Teams, and Combat Mission Teams
- DoD and DHS acquisition priorities

Register Now! Http://Cybersecurity.Dsigroup.org

The ways of making a Deep Web's content

Milica Djekic

Through a recent time, a Deep Web has attracted an attention of many security agencies and services due to its correlation with a criminal and terrorist community. A lot of people worldwide are getting familiar with this technology and many of them would use it on a regular basis for, more or less, legal, semi-legal or completely illegal purposes. In such a case, what we could identify as a key question here would be how it's possible to create a content for a Dark internet and why it's making its tendency to become bigger and bigger over a time. Through this quite comprehensive review, we would attempt to deal with these issues as well as leave some open questions within our concluding remarks to some future discussions and research.

How a Deep Web would work

A Deep Web is a internet content which is around 500-600 times bigger than a Surface Web. The Surface Web is a part of the internet that is indexable and queryable by standard search engines such as Google, Yahoo!, Bing and so on. [3] Basically, the both – a Surface and a Deep Web are the internet content which is stored into searchable databases, so it's possible to access them only if you have the right technology. [2, 6] As you know, a web business is nothing else, but rather some web content stored into databases somewhere on the web server.

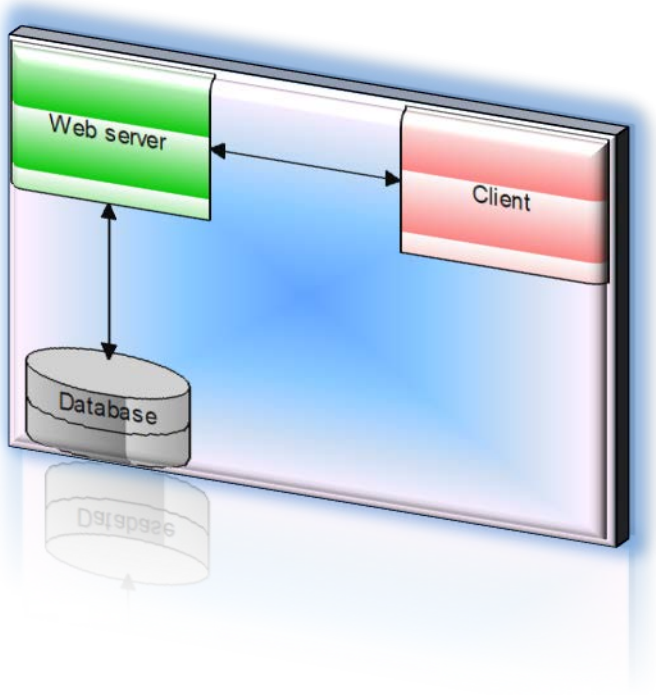
For instance, we could try to rely on some sources which we would find on the internet and which would claim a quite opposite things. Firstly, what dragged our attention was the question which sort of content would get included into a Deep internet. By some, the crucial difference between a Surface and a Deep Web is that those Surface Web pages are static, while the Deep Web pages are dynamic. [2, 3, 6] On the other hand, by another source, some of the modern search engines like a Google are capable to crawl even dynamic pages if their parameters are not change in terms to restrict so [4].

What we can notice here is those two quite reverse claims would come from so respectful sources, so we would not try to disapprove any of them, but rather suggest some future researchers or web developers to try to examine these claims in order to obtain some evidence which would be good enough to rely on them.

Is it hard at all to make a Deep Web content?

As everything else regarding cyber technologies, making a web content is just about playing with different parameters as well as opportunities that some web building tool could offer to you. From our practical experience, it's so easy to adjust parameters in, say, Wordpress or Joomla! and make your webpage, more or less, convenient for indexing or, more or less, friendly to your search engine's crawling mechanism. In other words, it's only about how skillful

a website builder is and how good he can take advantage over all the possibilities that emerging technologies would offer to us.



Right here, we would talk about how to create a dynamic web page which would, by all our sources, at least, make some difficulties to our search engines to crawl it. For example, a quite convenient way to make a web server for a dynamic website out of your computer is to use a XAMPP suite which could be downloaded for free from the internet. As we talked before, in order to store your web content somewhere, you need a suitable database. The advantage of using a XAMPP platform is that this tool would offer you all in one – an adequate database software as well as scripting language and, finally, web development environment. So, you would agree it's quite simple to make a web server out of your computer and hold your website content there. Next, everyone who would send a request from the web to your website would be called a client. As it's obvious from the figure on our right, once your web server gets a request from its web client, it would seek such an information from its database. Once it obtains that detail from there, it would return it to its client. A quite convenient and inexpensive method to maintain your website, right?

The trouble here would be that these all would be something that bad guys can do as well. They can simply download such a XAMPP application from the web and use it to make a dynamic environment for their webpage creating. Well, that's the problem for real, because once you create a Deep Web content, it's getting challenging to track such a web pathway. [1, 5] As it's known, in such a case, nearly the entire pathway, from a web server to a web client, is cryptographically protected. As we talked before, it's possible to access such a web content, but you need the right technology for doing so.

Why such an environment gets bigger through a time

The fact is the entire internet environment – earthier a Surface or a Deep Web is getting bigger and bigger over a time. [2, 6] This is especially significant when we talk about Deep Web technologies. What we've done here is a critical review on why we have such a tendency. Firstly, the internet connections are getting so suitable to everyone worldwide. At the moment, it's believed there could be nearly 3 billion people at a global plane capable to get online. Also, modern technologies are getting simpler and user friendlier over a time. It's easier than ever to gain a skill and get capable to make something on the web. So, as a second reason for such a raise of cyberspace, we would mention a simplicity and availability of emerging technologies to

everyone on the globe. Finally, it's so convenient making a web content and hold it on your private computer, a public web server or simply borrow a space on someone's else private machine for a very low rate.

Some concluding remarks

At the end, we would notice that there are still many open questions regarding this contribution. What we've done here is an attempt of some sort of a theoretical research which could not be assumed as comprehensive without an experimental effort which would offer a good opportunity to some future researchers to verify their claims and provide some real results that would rely on some sort of evidence. For such a reason, we would encourage the other cyber researchers as well as IT professionals to conduct such an investigation and try to provide more findings to this topic which, at this stage, we are not in position to obtain due to our limited possibilities and resources.

References:

[1] Peter Biddle, Paul England, Marcus Peinado, Bryan Willman, *The Darknet and the Future of Content Distribution*, Microsoft Corporation, 2002
[2] Bright Planet, *The Deep Web: Surfacing Hidden Value*, White paper, 2000
[3] *Deep Web (Search indexing)*, Wikipedia:
http://en.wikipedia.org/wiki/Deep_Web_(search_indexing)
[4] *Dynamic URLs vs. static URLs*, Google Webmaster Central Blog:
http://googlewebmastercentral.blogspot.com/2008/09/dynamic-urls-vs-static-urls.html
[5] Mohammadreza Khelghati, Djoerd Hiemstra, Maurice van Keulen, *Deep Web Entity Monitoring*, University of Twente, Netherlands, 2012
[6] Steve Pederson, *Understanding the Deep Web in 10 Minutes*, Bright Planet, 2013

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. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications. She writes for Australian and American security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

The New Security Rules Of Hadoop

Tackling Data 2.0

Jeremy Stieglitz, VP Products, Dataguise

The advent of Hadoop has introduced amazing new possibilities in data science for analytics, audit, fraud detection, and real-time prevention for cybersecurity teams. Hadoop's flexibility and speed means more logging and event data can be processed in more ways. Yet with this massive data influx, it can be difficult to account for all of an organization's sensitive data. Details such as network configurations, addresses, user names, passwords, location data can represent leaks and breach risk if they are not secured. And with more unstructured or semi-structured data muddying the identification and location of sensitive data, protection and managing risk in Hadoop has gotten even more challenging. This article will highlight some of the business and technology drivers for new security data management in Hadoop, and propose sensitive data discovery technologies to drive data-centric protection to address these.

Data 2.0 Forces New Security Thinking

Hadoop is much more than just a very large database. With big data, enterprises now have access to more data coming from a wide range of sources – like social networks – and are intent on better leveraging the value of this disjointed information across multiple applications. This endeavor has resulted in a major challenge in handling the volume, velocity and variety of structured and unstructured data. In terms of actually handling the data itself, there are 3 primary differences between traditional data repositories and Hadoop: type, access, and process.

1 – Type

Hadoop provides the ability to work with structured, semi-structured, and unstructured data. Massive scalability and this huge array of new data types in Hadoop has created a situation in which enterprises can no longer place guarantees on data being appropriately classified, provenanced, cleaned, and trustworthy.

In particular, businesses are increasingly combining web clickstream and application logging data (data historically too noisy or too voluminous to process in data warehouses) and combined with relational data or customer profiling data traditionally kept in the data warehouse to drive new business insights.

The presence of this "gray data" poses entirely new security challenges because the classification and/or location of data which may be sensitive is not known. Unlike database and data warehouse data models, where sensitive data can be catalogued and known in a more or less static data model, no rigid structure or sensitive data identification exists in gray data.

2 –Access

Enterprises today are more reliant on data than they have ever been. Decisions regarding attacks, forensics, product performance and operational characteristics are strongly guided by data. At the same time, data access and analytics are no longer limited to dedicated PhDs and cyber security veterans. Now business and technical users across finance, marketing, supply chain, engineering, project management, and sales operations want to analyze and improve decision making based on data mining and analytics. To maximize this promise of Big Data, businesses are making efforts to provide wide availability to data, and integrate and consolidate information silos throughout the enterprise. New tools are also provided dramatically easier business user access to data, in the form of sophisticated visualization programs, and expansions to everyday business productivity tools such as Microsoft Excel that allow non-developers to run queries and ask natural language queries of data. This expanded access and data consolidation has invariably decentralized data usage and grown the risk management and data governance requirements for IT. Enterprises now have the need to enforce greater control over how this data is made available to curtail risks of misuse within this larger context of data democratization and open access to enterprise wide data analytics.

3 –Process

Data processing in Hadoop is fundamentally different. Unlike data warehouse or database systems that store data and load data into applications and queries, queries and applications and now being brought to the data as computational processes are done at the data level or in real-time data streams. Most significantly, with real-time streaming rather than the traditional data model of storing, indexing and querying data, there is no data “at rest” per se as the data is used, analyzed, re-purposed before it’s ever stored. The security impact of this shift is large. The fundamental data encryption strategies around locking data “at rest” or “in flight” in a Hadoop environment break down. The more accurate data protection question may become: do you do encryption for data in-process?

Tackling Data 2.0 with Data-Centric Discovery and Protection

> By now, we’ve hopefully drummed home just how different data in Hadoop is. It’s vast, varied, and vague. It can be unpredictable, it defies order, and it’s very tough to govern. Not surprisingly, data breaches abound in this Wild West-like environment. They abound because traditional security tools have not adapted to the complexities of big data.
>
> Traditional security measures are built on top of newer big data technologies. This approach does not work because security must be implemented at a fundamental level in the design of a data security tool. Firewalls can protect sensitive information from external malicious access through IP and port checks without having any underlying knowledge of the network structure. Once that structure is breached, an attacker can access or steal any data in the Hadoop cluster. For example, an Access Control List (ACL) will not restrict user access if a data block is not deemed to be sensitive. In the Hadoop data model, this data block may be unstructured text or a stream of data that needs to be analyzed at the content level in order to be classified as sensitive.

Data-centric security — a strategy that precisely pinpoints, protects, and continuously inspects data at the element level — can address the risks of big data while preserving data accessibility across a broad user base and a variety of uses in Hadoop. By adopting a data-centric security strategy *in addition to* the traditional security tools, and organizations can answer fundamentally important questions about big data: *what kind of sensitive data is present across our enterprise?* and *where does that sensitive data reside?* After answering those questions, the right steps can be taken to protect sensitive data, using data use cases and enterprise privacy policies that work in tandem.

A data-centric security strategy can result in more accurate risk management, more flexible policies for data sharing, and critical visibility and precision within data structures including clickstreams, logs, user documents, and e-mail content that now have some of the highest growth rates in Hadoop.

Everything Starts With Discovery

Data-centric discovery for Hadoop allows businesses to detect sensitive data at the element level, so that organizations that are bringing Credit Cards, Social Security Numbers, Names, Addresses, Health Records, Financial Performance Results can determine where, how much, and how often these elements are found across the entire data store in Hadoop. Customers use discovery in five fundamental ways: visibility, as a means to protect data, as a means to count and realm how much sensitive data exists, as a way to risk profile and tie sensitive elements together, and as a way to continuously monitor data for changes or new risks.

Business Benefit	Hadoop Data Discovery
Visibility into risk	Discovery reports all sensitive data across entire Hadoop.
Comprehensive Coverage	Can run against data stored in Hadoop (HDFS), NoSQL (Cassandra/Datastax), Relational Data Management Systems (RDBMS), File Systems and Sharepoint
Real-time coverage	Can run in data-in-motion through agents for Flume, FTP, Sqoop, or Kafka (Summer 2015)
Protection of data	Automated protection policies provide options to encrypt (AES/FPE), mask, or

	redact sensitive data once discovered
Ability to count and realm sensitive data	100% automated discovery can run on all new data with reporting to determine the file / offset location of sensitive data elements and the size of sensitive data across all files and directories
Risk profiling and audit	Unique entitlement reports show who can access sensitive data in Hadoop
Monitor for changes, catch exposures	Monitor system for changes; can run as incremental scans

About The Author

Jeremy Stieglitz drives Product Management for Dataguise, the market leader in Hadoop security. Before joining Dataguise, Jeremy worked as Vice President of Business Development at Voltage Security, and as Vice President of Marketing and Product Management for Redwood Systems. He also held product management and marketing roles at Redwood Systems, Force10 Networks, Cisco, Entrust, and RSA. Jeremy has spoken at leading security conferences including the RSA Conference, InfoSec, Networkers, Connectivity Week, SuperComputing, SemiCon, and Internet2 and is the author of 19 patents in network security, user authentication, network automation, and wireless security.

Jeremy can be reached online at Jeremy@dataguise.com, is on Twitter at @BigDataProtect and www.dataguise.com.

GW's Cyber Academy

BUILDING BRIDGES *to* PROTECT CRITICAL INFRASTRUCTURES

Professional Training | Academic Programs | Applied Research

The new Cyber Academy at the George Washington University's Virginia Science and Technology Campus builds strategic partnerships with leading companies and public agencies, provides educational programs and training facilities, and offers applied research opportunities in the field of cybersecurity.

Professionals can earn a bachelor's degree, master's degree, or key certifications including CAP, CISSP, CISM, Ethical Hacking, and Security+, which are required by homeland security agencies, military, and cybersecurity industries.

To find out how GW's Cyber Academy can help you and your organization, please visit **cps.gwu.edu/gw-cyber-academy**.

For more information, please visit
cps.gwu.edu/gw-cyber-academy.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Detecting Cyberthreats "In Motion" Will Dramatically Improve Detection Rates

by Daniel Nieten, Ph.D.

As the world continues to generate a flood of information, governments, businesses and individuals understand that nefarious players are everywhere, waiting in the wings to wreak havoc, potentially on their organization's data assets. Whether for profit on the black market, to undermine national or international security, or to obtain intellectual secrets, the threat of a cyberattack is real and inevitable, making cybersecurity one of the most important issues of our day.

Yet despite massive amounts of spending on cybersecurity solutions, the frequency and complexity of breaches continues to increase and the cost in the aftermath of a breach has skyrocketed. With increasingly sophisticated blended threats, combined with massive data volumes that create scalability and speed issues, it's understandable why the ability to detect a breach has been so elusive, and why detection times are so long. According to security firm Mandiant's 2014 Threat Detection Report, the median number of days that a threat was present on a victim's network before detection was 229 days.

Simply put, organizations don't know what they don't know, they can't see what they can't see, and as a result, they cannot detect—much less respond to—an anomaly or potential threat that they don't even know is either coming at them or already in their system.

Immediate threat detection requires the ability to take in all the information emanating from an organization's many data feeds throughout its entire enterprise infrastructure, all at the same time, all the time, and bring it into one simplified, unified view. Then, that data must be acted upon when it initially becomes available and while it's still moving in the system—or what we call "data in motion"—in order to surgically pinpoint and immediately bubble up to the surface a potential anomaly or behavior that could pose a threat.

Technology that is architecturally designed to process "data in motion" is able to ingest everything—i.e. all the data along with its context, from all of the disparate data feeds found in a typical organization's IT infrastructure: routers, firewall, IPS, antivirus, SIEM, syslogs, netflow, switches and more. Then, leveraging advances in artificial intelligence and machine learning, the analytics are performed on the fly, creating correlations that can identify a potential threat to the network. Every component of such a system is created to act on the data before it ever comes to rest.

This is very different than the majority of the systems in use today, which rely on an "analytics-after-storage" model where data is gathered and stored in a database. Then, analytics is performed in batches, but after the data has been persisted —or has come to rest.

This model claims to be real time, but only the ability to query a data repository is real time—or as the user is waiting, in reality the analytics becomes forensic in nature. Data that has already come to rest has an inherent latency and does not give organizations the vital rapid detection edge they need to stop an attack at its onset.

It takes extraordinary computing power to handle the unprecedented volumes and types of data flowing into to the typical enterprise infrastructure, where organization are geographically distributed, with people and offices around the world, operating devices that allow them to enter the network from anywhere, anyplace, at any time.

It also requires the application of new advances in correlation and algorithmic technology so that organizations have the correlated results available. This provides the ability identify patterns and detect anomalies without any rules or signatures. To date, the majority of existing systems have been highly dependent on identifying known threats—those based on a signature or rule—despite the fact that many of today's threats are never-before-seen attacks, the "unknown unknowns."

Technology that can ingest, analyze, index and correlate massive amounts of data from disparate data feeds, while that data is still in motion, will enable organizations to rapidly detect anomalies, identify whether or not they are a threat, and then automate client-determined remedial actions.

Data is a fluid, moving entity. It is constantly in transit either into, out of, or within an organization. To protect and defend data assets, companies need the ability to see what is happening to data *while it is moving and in transit*. Technology advances are being implemented today that will begin to dramatically shift the breach detection paradigm by giving companies the ability to detect a potential breach faster than ever before possible. While we may never be able to thwart every potential threat, we most certainly have the technological capability to drastically reduce detection times from months to just a few minutes. We just have to embrace them. When we do, the balance of power will finally shift in our favor.

About the Author:

Dr. Dan Nieten is the Chief Technology Officer for Red Lambda, an award-winning cybersecurity technology company. The company's flagship solution, MetaGrid, is an advanced, software-based cybersecurity system designed to protect commercial and government enterprises by identifying anomalies and threats "in motion" at detection speeds never before possible, without rules or signatures. The company is headquartered in Orlando with offices in the UK.

Keeping up with the complexities of malware

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

Reading through news and opinion sections on IT-focused blogs and websites, it's not uncommon to come across assertions like, "the threat landscape is growing more complex/fast-paced." Certainly, this isn't news to anyone, but what does it actually mean?

A group of researchers at G DATA recently released the results of a study that may give some clarity here.

According to the report, G DATA found that in 2014, almost 6 million new strains of malware came to the attention of the security community.

Of the 6 million, researchers found 4.1 million of them in the second half of the year alone. For comparison, only 3.4 million new kinds of malware were discovered throughout the entirety of 2013.

Adware Stands Out in the Rising Tide of Malware

The complex nature of today's threat landscape is tied to the endless wave of new malware variants security teams and their tools have yet to discover. When one considers that most security solutions can only protect networks from known threats, it's clear that organizations are at risk of being overwhelmed.

The report furthers that among this increase in new malware, adware has grown to be one of the most prominent types.

A recent *CSO* article defined adware as, "…malware that infects existing ads to cause malicious downloads, force intrusive popup ads, and plant additional malware on a user's system, leading to a data breach or attack on critical systems".

Banking Trojans Out of Vogue

The rise in malware coincides with the decline in the use of banking Trojans, which are geared toward stealing financial data from banks and other institutions.

The G DATA report stated that the number of targeted banking Trojans dropped by 12-percent in 2014, which may be a function of the increased attention and better security that the financial industry has enacted over the last few years.

Per the CSO article, head of G DATA SecurityLabs Ralf Benzmüller theorized that, "Improved security measures by banks are making it more and more difficult for online bank robbers to get money from bank customers."

Because banking malware is less likely to succeed in the face of bulked-up security, hackers are turning to new tactics, like adware, which could have a better chance of penetrating cyber defenses.

With so many new types of malware, it's unlikely that perimeter defenses can stop them all.

Organizations that adopt a layered approach to security, with a new emphasis on automated threat detection and removal, will be better positioned to ward off the myriad threats they face.

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

Digital and Physical Security - What Every Small Business Needs to Know

Your small business is your bread and butter. If anything happened to your business's assets, this would leave you and your company in financial and possibly legal straits.

From high-end equipment to the security of personal information for all your clients, there is a lot of assets to protect that are central to your company's ability to do business.

Additionally, it is critical for your company to maintain a reputation that is, in a word, exemplary.

For these reasons, it is essential that you protect your small business with multiple layers of physical and digital security.

The following are some things every small business should be aware of when employing various types of digital and physical security measures.

Encrypting Data

Data encryption is an important measure when it comes to protecting everything from company secrets to the personal information of all your important clients.

Even if you think your company's VPN is protected with an array of sophisticated firewalls, all it takes is for a clever hacker to slip in under the radar and compromise your company's stored data. The point of encryption is to complicate a hacker's efforts.

Even if they get their hands on your company's precious data, their ability to read or use that data is dependent on whether or not they can crack the encryption measures you have used with which to obscure the data in question.

Dedicated Computer Access

When it comes to protecting your company from having its financial information hacked, it is important to consider only using a single computer in order to access financial information. This is both a physical and digital method of securing your company's financial records and liquid assets.

With only one computer being used in a dedicated way for this purpose, you essentially restrict the number of employees who would have access to such information. This in turn reduces the potential for an internal breach of sensitive financial data and account information.

If a breach happens, it is typically going to narrow the number of suspects down to a very limited list of people that need to be investigated or further observed.

Cameras Cameras Everywhere

With as cheap as it is to install an array of cameras around an office, it is a wonder more small businesses fail to implement this simple security strategy. Multiple cameras will provide a business owner with the ability to monitor everything happening inside and around their company's building.

With motion sensors and mobile apps to access cameras by remote, it is a simple matter to oversee everything going on from the convenience of a smart-phone or phablet from anywhere where WiFi access is available.

There are many different companies that provide this type of service, some of them are more specialized such as Pro-Vigil, while others are not specific to certain types of companies. This is also a way to ensure that an employee is not trying to access parts of your office that they are not permitted to enter.

Any attempt to break into the bosses office, for example, immediately triggers a motion-sensor camera that sends an alert to the bosses' mobile device.

Adding a Security Detail

It is the middle of the night and a burglar is attempting to gain access to your office building. Fortunately, you decided to hire a security detail to monitor the halls and entryways.

With the push of a button and a word or two over a radio handset, every member of your private security team converges on the scene to apprehend any threat to your company and its assets.

Such a measure may seem excessive for some small businesses, but it really depends on how likely of a target your business is to thieves and how expensive the assets are that you are attempting to protect.

This is a form of cost analysis that an owner of a small business may need to take into consideration to determine if their business needs warrant hiring security guards for on-site monitoring purposes.

It is important to remember that people are capable of adding intelligent decisions to a small business's security measures beyond what a machine can provide.

About the Author:

Lee Ying has over 10 years experience in the tech and security industry. He currently writes for various websites, if you would like to contact him you can find him on LinkedIn: https://www.linkedin.com/pub/lee-ying/9a/18b/238. Follow me on Twitter @LeeYing101

Protecting Yourself After a Massive Data Breach

Hackers and cybercriminals are coming up with more and more devious ways to steal every day. Some of the data breaches are huge, like the attacks on Target and Anthem, allowing hackers to get access to millions of social security numbers, email address, credit card numbers and other personal information. Some are state-sponsored cyberattacks, like the recent massive data breach that affected virtually every U.S. government agency. All the above increases the risks for identify theft on a global scale.

Victims of identity fraud can take steps to notify the authorities and credit bureaus. Massive data breaches are different. Being part of a data breach is like losing your wallet at the mall -- no way to tell who has it, how they will use it, when they will use it, or if they will use it at all. Only one thing is certain: you must take precautions.

Max Nomad, IT computer consultant and author of the book **Surviving The Zombie Apocalypse: Safer Computing Tips for Small Business Managers and Everyday People** offers up specific advice:

1) Perform a deep scan of your home computer(s) using multiple antivirus and malware removal programs. Massive data breaches mean that numerous computers were affected, including privately-owned machines. Take steps to make sure yours is clean before proceeding with step #2.

2) Change the password(s) to every account on your home computer. This should also include your home WiFi too, both the administrator password and the connection passphrase.

3) Get a Password Locker app and use it to generate and store all your new passwords. Your new passwords should be

- at least 12 characters long,
- use upper and lowercase with one or more numbers and special characters,
- does not use proper names or words from the dictionary,
- unique (as in not used for anything else), and
- stored only in a Password Manager app (and never stored in your web browser)

4) Go through and change the passwords to every online account. Online banking, online payment sites, etc. This should include changing your secret questions and answers. I would also recommend changing all work passwords but their IT departments are going to make that happen anyway.

5) Clean your browser history regularly. If past passwords were stored in the browser, clear them out and don't replace them with your new passwords. Although the "Remember password" feature is convenient, hackers know how to retrieve passwords from these caches.

6) Enable two-factor authentication everywhere possible, starting with anything related to

banking and credit cards.

7) Make sure your emails are not being tracked. Tracking uses one or more images in an email to geo-locate where the message is being viewed. Disabling images in your message previews prevents this kind of tracking. Any messages you don't trust, delete them instead of allowing them to download and display images that are part of the message.

8) If you don't have a public key, go to https://gnupg.org , download the software and create one now. Aside from being able to send and receive securely encrypted emails, these can be used to digitally sign your public messages to verify that these posts came from you.

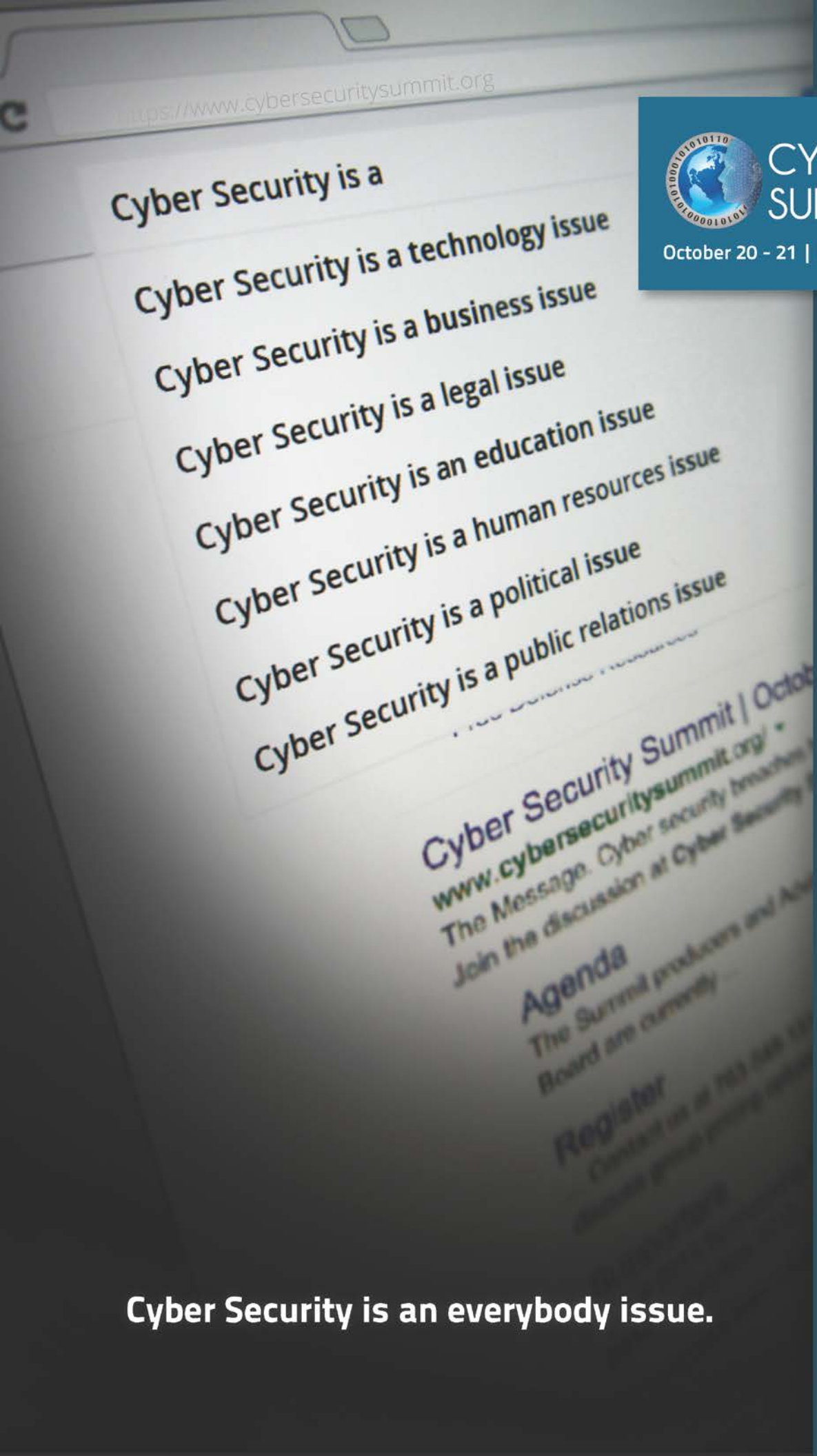
9) Notify your business associates, friends and family of the fact that your information may have been compromised in the data breach. Make sure they understand you might be digitally signing your online communications.

10) Be vigilant, both with your online communications as well as phones.

There are other precautions that can be taken but most of them range from the obscure and inconvenient to the extremely paranoid. For more no-nonsense cybersecurity tips for the layman, check out **Surviving The Zombie Apocalypse: Safer Computing Tips for Small Business Managers and Everyday People.**

About the Author

Max Nomad is an IT Consultant, Graphic Designer, creative entrepreneur and computer security researcher with over 20 years of experience using Internet technology to assist (and protect) small businesses. Having worked with everything from stock brokerage firms to car dealership chains to ostrich farmers, his diverse client history has given him experience with a variety of large and small business needs. He also writes candid and informative essays focusing on publishing, graphic design and the underground side of cybercrime. He lives in Virginia Beach, Virginia and can be reached at nomad@beach-geek.com.



CYBER SECURITY SUMMIT 2015

October 20 - 21 | Minneapolis Marriott Northwest

Today's security challenges can't be addressed by one sector alone — they require public-private collaboration and a commitment to action from all stakeholders.

Come to the Fifth Annual Cyber Security Summit to engage the issues with an audience of C-level executives, technology leaders, risk managers, policymakers, lawyers and more.

WHAT TO EXPECT:

- Higher-level strategic and systems view
- Open, off-the-record discussion
- Strong partnership with the government and private sector
- Experts from all aspects of the solution
- Meaningful conversation about both strategy and tactics
- Thought leaders from multiple global cities

REGISTER NOW TO SAVE

Attend the full Summit for $499 with early registration pricing.

Cyber Security is an everybody issue.

www.CyberSecuritySummit.org

Regionally Focused Security Lessons on Tap at RSA® Conference APJ

RSA Conference Asia Pacific & Japan 2015 will feature many top-rated speakers from across the globe delivering powerful presentations. The Program Committee has had its hands full this year as it sorted through a record number of submissions, tasked with selecting those that provided the most timely, compelling content for our attendees—content that would really change the way they do their jobs and secure their organizations.

We are extremely pleased with the nine-fold increase of submissions this year featuring research and analysis specific to Asia. This will help us deliver on our promise of delivering a RSA Conference APJ with programming that directly matters to our local attendees.

A few months ago we analyzed the 2015 U.S. submissions and uncovered a few patterns which we were able to map to overall security trends. We applied the same type of analysis to APJ submissions—utilizing the above word cloud and other data analytics—and found the potential speakers were focused on similar topics as their US counterparts, but through a regional lens.

We have presenters who will provide a detailed analysis of threat actors and techniques used to target Asian organizations—who, incidentally, are targeted more frequently than their Western counterparts. Detailed presentations about specific hacktivist and nation state attacks will also be delivered with in-region examples and data. The ability of our presenters to hone in on the direct and distinct needs of our local audience is exciting for us to see. The details and insights will help our attendees realize tremendous value by attending this regional event. Similarly, we saw a marked increase in session submissions that discussed specific breaches and threats. Based on the levels of increase, we seem to have crossed the threshold where, to use a phrase

that has now become all too trite, organizations no longer wonder if they'll be breached but rather when…and how often.

Our submissions show the conversation has turned a corner, with a willingness to share real lessons (another word that showed up considerably more often in the 2015 title word cloud vs the 2014 title word cloud) and specific steps organizations have taken in response to the changing threat landscape. We are poised to capitalize on real information sharing and experiences.

One of the most consistent pieces of feedback from the 2015 US Conference, contrasting past events, was that this year sessions focused on "real, tangible, directly applicable things I can do to better perform my job and protect my organization." There was a real sense of empowerment and, dare I say, excitement across the week that was reflected in feedback as attendees appreciated sessions weren't just focused on "what's wrong…and that's bad", but rather solutions and experiences. RSA Conference APJ looks to match that same experience for our attendees based on the lessons and perspective reflected in the submissions.

Rounding out our big trend increases, as observed through submissions, is the Internet of Things (IoT). The interconnectedness of everything is clearly on minds as submitters explore the implications of this brave new world. In region our submitters observed the impact of the IoT on cloud and mobile approaches and processes, both strong areas of focus in region—even more so than in the US, as evidenced by their steady hold as a percentage of submissions.

Topically we saw certain distinct declines this year in submission as well, all three of which seem to support a maturation in how organizations approach security.

- The number of times Bring Your Own Device, or "BYOD," appeared in submission titles declined significantly. This seems to be a product of organizations just accepting external devices coming into enterprise networks and, vice versa, enterprise tools being used on home networks. Organizations seem to have evolved in their concept of what they need to be aware of and protect and no longer look at BYOD distinctly.
- Likewise, APT as a distinct term seems to have peaked (globally) last year. Recall that "threats" as a general category is up—way up in APJ—but the distinction of different threats as more (or less) advanced than others seems to be on the decline.
- Lastly, as with a trend we saw in the US, the focus on compliance seems to be down. A compliance dismissive tone seemed prevalent. Perhaps the breaches of 2014 established clearly that compliance does not equal security. It's an interesting shift from past years.

There you have it—what's trending up and trending down in APJ, as analyzed through the RSA Conference APJ submissions! We are extremely excited about the content to be shared and its direct applicability to our Asian Pacific-based attendees. Please follow our Quick Looks and early deck postings to assure you're in the best position to get the most out of this year's presentations.

There's an App for That, but what About Security?

By Mav Turner, Director of Business Strategy, Security, SolarWinds

It's no secret that in today's uber-connected digital world, a growing number of organizations are experiencing the crippling impact of cyberattacks and data leaks. Following several recent and high-profile incidents, everyone is a-buzz over the importance of securing infrastructure and data to avoid a breach.

But these conversations neglect a vital component of true enterprise security—the applications that run on these networks and devices, which have their own set of unique vulnerabilities that can ultimately be the single domino that topples an entire enterprise security strategy.

Although the "there's an app for that" mentality has spread to penetrate both our corporate and consumer lives, the concept of native app security is still largely unexplored.

Apps often demand custom security measures, and in the absence of an easy to apply blanket solution, many developers are prioritizing speed to market over finely tuned secure technology.

So what's the solution? Think of it this way: app development should be approached with the same considerations as a contractor building a house.

The very foundation of the app, security, is much more simply integrated if done at the get-go, rather than as an afterthought—similar to a builder installing key utilities, like plumbing or electricity, during the construction phase versus making those changes years later during a costly renovation.

Moreover, when security measures are applied to agile methodology and innovation, developers should establish checkpoints at each stage or iteration to ask themselves, "Could I break this?"

After all, like a builder, the farther you get into development, the more difficult—not to mention expensive—it is to backtrack and fix something that was flawed from the start.

With this in mind, here are several key considerations and strategies that organizations can leverage for safe and secure enterprise app development and deployment.

1. **Take a lay of the land.** Begin your process by dedicating time to understanding and defining what app security will look like for your organization. Organizations building a simple Web-based app will need significantly less security than a business aiming to run an app designed to store confidential customer or personally identifiable data.

   A useful exercise when building an app or even simply evaluating your organization's security needs as a whole is to imagine how detrimental a data breach through a

particular app would be to your organization. For example, what do you stand to lose if an attacker, in a scenario similar to this year's Anthem data breach, achieves higher access privileges and secures long-term access to your data? In Anthem's case, just five cracked network user IDs resulted in the loss of the personal information of over 80 million people.

So, ask yourself, "What data is the app storing and/or processing? Who has access to that data? What security measures are in place for approved users? If an employee loses a mobile device, does the network require a VPN password for remote access and if so, is that password cached?"

To best inform the approach you take to security policy, having a firm grasp of the types of information that is stored, shared and accessed on these apps is critical.

2. **Build a solid foundation.** It's been proven that when coding to secure an application, "default denying" everything throughout the design process will ensure an application is sufficiently protected. In addition, assigning permissions as needed will make it much easier to pinpoint the source of a vulnerability if and when it occurs.

   The key to getting your app to this point requires there be a heavy focus on security from the outset of its development so as to be properly integrated throughout each phase.

   From a design perspective, while user interface and user experience are key considerations in the evolution of any app, they are also intrinsic to security. Every effort should be made to take the weight of security responsibility off the end-user's shoulders.

   Why? Because if an app requires the user to make a decision between security and convenience, it should come as no surprise that they would more often than not default to convenience—and in many cases, this decision presents serious consequences for your organization.

   In those instances when you're forced to compromise convenience for the sake of security, such as repeated, required VPN log-ins, a user should be made aware of and understand the security reasoning behind that decision.

3. **Prepare for anything—and that means the worst.** Even with a heavy cover of policies, if you don't have a plan within those policies or if your team doesn't fully understand it, your organization is at risk. It's especially worth noting that many IT Pros and developers may wonder why investing in native app security is necessary when the organization's core infrastructure and shared platforms could be locked down instead.

   At the end of the day, if your business is running apps on shared infrastructure, you have to assume these platforms aren't secure and the possibility of data being leaked is very real.

Take Target's 2014 data breach, for example, which was made possible via a small heating, ventilation and air conditioning company tasked with remotely monitoring energy consumption and temperatures at various Target stores. Hackers were able to leverage the company's access credentials to move about undetected on Target's network and upload malware. Ultimately, anticipating and planning for disaster means operating under the assumption that someone is always watching your network, your infrastructure and what passes through it, internal or external.

Additional considerations for developers working closely with an internal IT infrastructure team or cloud provider include understanding what their SLA policies are, how often they update them, how often they validate them and whether or not they use auditors. Equally important is assessing what you know and don't know about a vendor's security history. What is their response time if they or a customer detects a vulnerability? What have they experienced before? They should have their own policy in place and have proof that it works. Your app may be secure, but the information or platform it sits on may not be, requiring a multi-faceted, layered security strategy.

With applications fast becoming the center of many organizations' business strategies and data breaches on the rise, placing a larger focus on enterprise security is paramount.

By keeping these three considerations top of mind, in conjunction with a ground-up approach to app security design, you can be confident that you're engaged in safe and secure app development, hopefully resulting in fewer instances of data loss.

About the Author:

Mav Turner is responsible for the SolarWinds IT Security business and product marketing team. He has been at the company since 2009, where he joined as a senior sales engineer.

Information Governance Exchange

September 14 - 16, 2015 • Gaylord Convention Center National Harbor, MD

Taking a Strategic Approach to Information Governance, Aligning IG Investments to the Broader Business Technology Agendas

Thomas Mavroudis, Chief Data Officer, Americas, Global Head of Data Quality, **HSBC**

Talvis Love, Chief Information Security Officer, **Cardinal Health**

Justin Skelton, SVP Data Management Executive, **Bank of America**

Mark Bisard, VP & Senior Counsel – Cyberlaw, **American Express**

Jeewon Kim, Chief Privacy Officer, **Fannie Mae**

Gerhard Cerny, Chief Information Security Officer, **AmerisourceBergen**

Rachel Reid, Senior Counsel and Chief Privacy Officer, **Voya Financial**

FIND OUT MORE

Visit: www.informationgovernanceexchange.com
Email: info@thelegalexchangenetwork.com
Call: +44 (0)207 368 9484

Top Tips in Information Governance

The Information Governance Exchange has interviewed the CISO, Cardinal Health, Chief Data Officer & Head of Business Intelligence, Toyota Financial Services, CISO, AmerisourceBergen and MD, Knowledge Strategy Solutions to give you their top tips in information governance. Read on to find out about hot topics such as the cloud, how the market has changed, establishing an IG framework, policy compliance, the new rule in auto deletion and much more!

Why Cloud is Important to Integrate from the CDO & Head of Business Intelligence, Toyota Financial Services

I don't believe we have a scope today. I think that people don't want to take the risk and to maximise the return of investment on data we have to be in the cloud – the cloud cuts the cost of maintaining and operating and using data – we can store data that otherwise we could not find easily.

Want to find out more about the cloud? Read this free whitepaper *Not All Clouds Are Created Equal* to discover more the various cloud services models that are best suited for managing important business information subject to governance, compliance, legal and business requirements.

Unified Approach from the CISO, Cardinal Health

Information is critical to running the operations and driving the strategy for our business. As such having a comprehensive view on data and information is essential to achieving the goals and objectives of both.

Find out more about created a unified strategy in this exclusive eBook: *Building Information Governance Across Your Organisation: The Data Privacy, Legal and Information Security Perspectives* where you will hear from a range of information governance stakeholders who offer insights into the role of information governance, the challenges facing companies in this area and advice on the solutions available to assist them.

How the Market has Changed from the CISO, AmerisourceBergen

The main difference is that there was a push to open the exchange of information in B2B of healthcare service and the interconnection of how do we get the information – how do we improve the services for the patients? Behind the scenes this means how do we interconnect, exchange, share and support the integration between many layers of the industry and the solution providers. This is quite a challenge because of the many standards that are involved especially from a global prospective.

Auto Deletion from the MD, Knowledge Strategy Solutions

In December 2015 we will be getting a new rule in the federal courts regarding sanctions – basically, under the new rules, the court will have to make a finding that the data loss occurred because the party intended to deprive another party in the law suit of the information's use in

the litigation. It would be extremely hard for any litigant to prove that a routine deletion pursuant to policy occurred "with an intent to derive.

Find out more about the new rule in this exclusive whitepaper which analyzes ways in which an organization could convince a federal court that an auto-delete policy was not intended for the deprivation of information required in the litigation, including auto-deletion intervals together with diligent litigation hold processes.

Data Management tips from the CDO & Head of Business Intelligence, Toyota Financial Services

The benefits of having an integrated approach to data management comes from having the right balance between data supply chain, the risk associated with it and the return of investment. If we don't have a good foundation we are going to have a hard time, meaning if you are more focused on risk or more on innovating you are not going to extract the maximum value from it, and this is all about governance!

Get more data management tips in this presentation about how DHS created a "data lake" to better manage all the information in one place.

These comments were taken from an infographic created by the Information Governance Exchange download the infographic here to find out the remaining top tips including **policy compliance**, how **vendors** are keeping up with the **rapidly changing market**, what these IG leaders think is currently **missing from the solutions market** and how Cardinal Health, Toyota Financial Services and AmerisourceBergen choose solutions!

These topics will be discussed at the Information Governance Exchange taking place September 14-16 Gaylord Convention Center National Harbor, MD. If you have a solution which helps companies improve their information governance strategy then download your information pack here email info@thelegalexchangenetwork.com or call +44 (0) 20 7368 9484 to find out more about how you could meet **80 SVPs, VPs** of **Information Governance** plus leading **CISOs, Chief Privacy Officers** and **Chief Data Officers** specifically chosen and screened to ensure that they all have an **active requirement** and are looking to **invest in the next 6 to 12 months.**

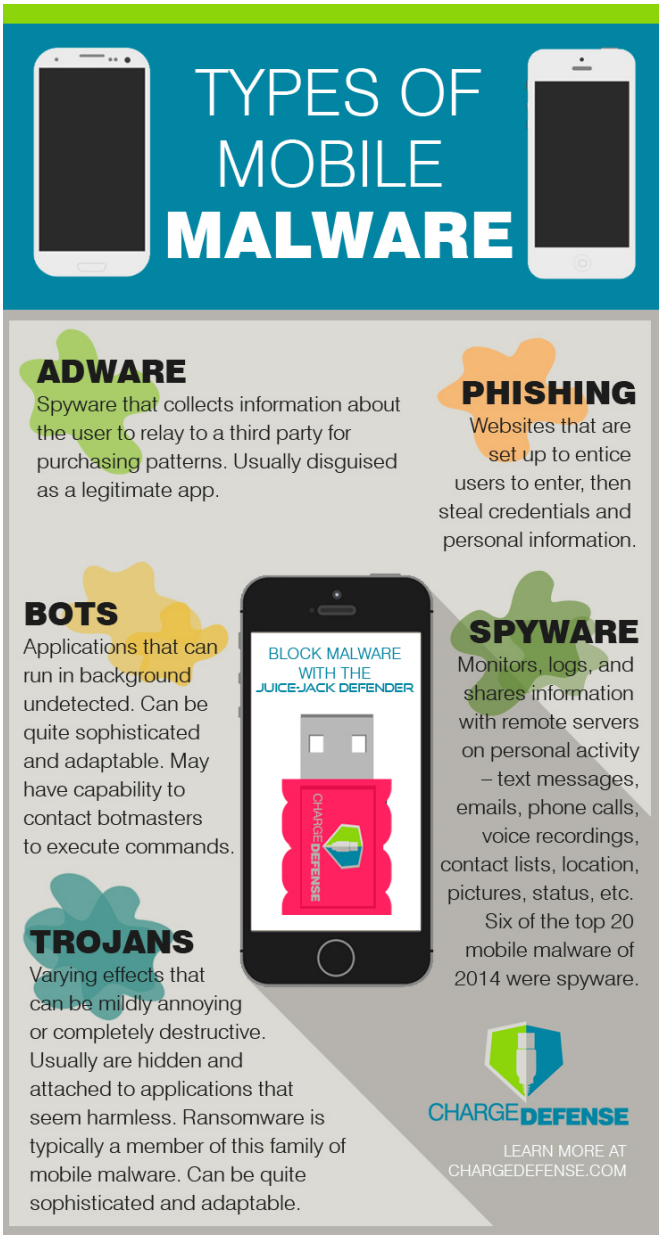
If you're in charge of your company's information governance strategy and are **interested in attending** the Information Governance Exchange then take a look at the agenda to find out more about the topics covered or request your invitation and one of the team will be in touch.

Information Governance Exchange

ALERT: SmartPhones – Twice as Dangerous as USB Flash Drives

Every IT professional knows that USB storage devices such as flash drives are notorious for carrying malware and exploiting USB autorun features to expose viruses to corporate enterprises. In fact, a Microsoft study in 2011 on 600 million systems revealed that malware infections via USB storage devices were responsible for 26% of the total infection rate[1], and that rate steadily increases year-to-year.

In 2014, Microsoft further showed that 5 out of 10 malware instances are worms spread by USB removable drives.[2] That astounding number of potential infections has led many IT departments to outlaw the use of USB flash drives on enterprise-connected machines. Nevertheless, infection rates through USB continue to climb.



Perhaps a major reason for the increase in and severity of these infections is the pervasive use of smartphones for consumer and business purposes.

After all, a smartphone is a USB storage device with a LOT more capability both for good and malicious purposes. Smartphones can not only carry around a virus (along with your personal information), they can also execute the virus on the phone itself, AND they can communicate wirelessly with the cyber criminals that put it there.

Yet most people never think twice about plugging their smartphones into any USB port within reach for a quick charge, especially while traveling.

It should therefore be said at shouting level: **SMARTPHONES ARE AT LEAST TWICE AS DANGEROUS AS USB FLASH DRIVES!**

Even Hollywood is picking up on the increasing trend in juice-jacking and understands the severity of having your

[1] Microsoft Security Intelligence Report Volume 11, January-June, 2011
[2] Microsoft Security Intelligence Report Volume 17 English, multiple authors, Page 97, January – June 2014

personal information hacked on your smartphone. A recent CBS CSI Cyber episode is centered around a cyber-criminal juice-jacking attack at an airport, exposing thousands of unsuspecting travelers to identity theft.

But, juice-jacking is not limited to connecting to unknown charging locations. Personal and corporate enterprise systems are just as likely to be both carriers of juice-jacking viruses as well as victims. The Stuxnet virus that hobbled the Iranian nuclear weapons program in 2010 is a great example of a targeted cyber-terrorism campaign which worked magnificently.

Cyber Terrorists Target Corporate Enterprises via Infected Mobile Devices

In the past couple of years identity thieves and hackers have become even more sophisticated, shifting their attention to mobile devices. Malware applications originally developed for Windows operating systems are rapidly being migrated to attack mobile platforms.

A February 2015 report from McAfee showed a 6x increase in mobile malware over a two year period and found that 8% of all mobile devices are infected with 387 new threats every minute, or more than 6 every second."[3] If you believe Cisco estimate of 4.9B mobile devices, then that is astounding 392M infected devices in the world.

McAfee further reported accelerated mobile infection rates with 17% growth in just the last quarter of 2014.[4] Alcatel-Lucent's Kindsight Security Labs report agrees with this staggering increase in mobile malware, stating growth of 20% in 2013 and another 25% in 2014 and growing quickly.[5]

The same report showed a nearly identical percentage growth of infections on fixed networks. The coincidence is interesting and illustrates how cyber criminals are targeting mobile devices to ultimately attack networked systems within corporate enterprises.

To further substantiate the concern of USB devices being used to infiltrate enterprises, the February 2015 McAfee report makes some very disturbing correlations on the recent Sony Pictures Entertainment master boot record wiping attack by North Korea.

They state that "this vector of attack [Shellshock] will be the entry point into infrastructures from consumer appliances" (connected devices like USB flash drives and smartphones) to corporate enterprises, and they "expect to see a significant increase in non-Windows malware in 2015."[6]

Although Android and Windows systems are the most common malware targets - nearly equally distributed at 50/50[7] - Apple iOS devices also have recently been targeted and infected by cyber criminals.

The Wirelurker virus infected desktop and laptops by posing as a popular game app that used USB ports to infect Apple mobile devices when connected to the infected machine. The mobile

[3] McAfee Labs Threats Report, February 2015
[4] McAfee Labs Threats Report, February 2015
[5] Motive Security Labs malware report H2 2014, Alcatel-Lucent, 2014
[6] McAfee Labs Threats Report, February 2015
[7] Motive Security Labs malware report H2 2014, Alcatel-Lucent, 2014

virus then stole information from mobile devices and sent it to criminals via wireless means. Apple responded rapidly by posting an operating system fix -but not before reports of hundreds of thousands of people had been infected, via the reactive "closing the barn door after the horse has escaped" process which all too many malware remedies end up following.

This wasn't the only major attack against iOS systems; 'Find and Call', discovered in 2012, was the first notable non-jailbreaked iOS trojan which uploaded contact lists to a remote server. Two years later spyware applications XAgent and MadCap were discovered on iOS systems.

This malware was directed at political and military employees and intended to perform advanced political espionage. This is not meant to impugn or blame Apple for product flaws; they are a great company with great products and, truth be told, they have much lower infection rates than Android devices.

However, it shows that no one is immune to mobile viruses. Everyone should be on high alert.

Protect the Enterprise from Cyber Criminals

So, what can IT professionals do to protect their Enterprise from inside threats presented by USB vulnerabilities which are often introduced unintentionally by well-meaning employees?

Educating employees on the dangers associated with USB charging is the first step. Implementing security policies and periodic training is a common best practice among most companies large enough to support an IT staff.

However, education, training and policies might not prevent an employee with just 5% charge left on their phone from plugging it into a USB port on his work computer. This small and seemingly harmless act can bring down an entire network if lurking malware on the phone can circumvent policies intended to thwart it.

Just as bad, it can also expose corporate intellectual property such as research, product plans, employee records, financials, and a host of other information that should never go outside of the corporate network.

The majority of USB enterprise security breaches are accidental. Therefore, more comprehensive mitigation strategies should be considered. One such strategy is the USB port blocker, which are inexpensive mechanical plugs that physically prevent the connection of all USB devices.

While this will work in some scenarios, the port blocker comes with an obvious disadvantage: it completely disables the functionality of the USB port, including its ability to charge devices. For the proverbial employee low on smartphone power you'll need to consider a solution that meets their needs as well as your security requirements.

It's possible to disable the data synchronization component of a USB port (which is how viruses can spread) while still allowing charging. Some devices and "charge-only" cables allow power-

only connections by disconnecting the data lines on the USB port. Unfortunately, this is not a solution for many more sophisticated smartphones, including the Apple phones, as they will not charge in this situation.

Other charge-only solutions charge at slow USB 1.0 speeds and may not support all mobile devices (smartphones and tablets) and mobile operating systems (Android, iOS, Blackberry, and Microsoft) or use chips that could potentially be hacked and completely defeat the purpose.

ChargeDefense's Juice-Jack Defender® is the solution that supports all these requirements – it blocks all data transfer between device and charging source, supports all mobile devices and operating systems, supports charging at up to twice the normal USB charging speed and has no chips or memory to execute and store malware.

The bottom line is that the majority of enterprise infections come from inside the company and most of those infections are unintentional. Over ¼ of infections are through USB connections and the trend with hackers and malware developers is to target mobile users.

Every smartphone should be considered an infected device when connected to enterprise machines. Simply implementing policies to disallow USB connections is not 100% effective.

A combination of education and training, port blockers, and power-only charging solutions such as the Juice-Jack Defender® is an inexpensive, practical way to keep honest employees from infecting your enterprise and exposing corporate and employee information to the bad guys.

Don't Get Juice-Jacked!

Sponsored By
THE WALL STREET JOURNAL.

Media Partner
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER SECURITY SUMMIT 2015

Moving Your Business Forward

D.C. METRO AREA
JUNE 3
The Ritz-Carlton Tysons Corner

NEW YORK CITY
SEPTEMBER 18
Millennium Broadway Hotel

BOSTON
OCTOBER 21
Back Bay Events Center

These "Invitation-Only" events connect Senior Level Executives with the world's leading Cyber Solution Providers & Thought Leaders

For Business Development Opportunities Contact Bradford Rand
at **212.655.4505 ext 223** or **BRand@TechExpoUSA.com**

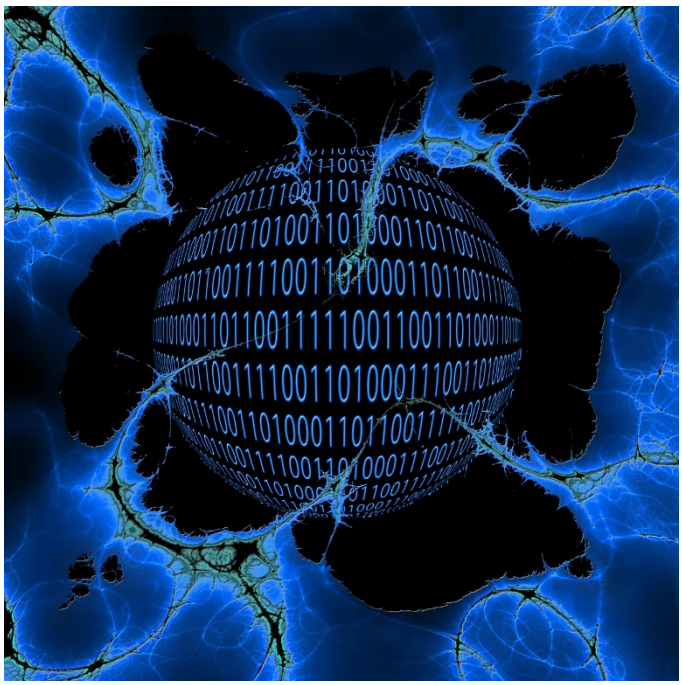
www.CyberSummitUSA.com

OPM Breach Highlights Need for Continuous and Contemporary Security

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

News of the attack on the U.S. Government's Office of Personnel Management (OPM) has appeared far and wide. As a result of this attack it is believed that personal data on 4 million current and former federal employees was stolen. Many of these comments I've seen or heard on the topic sound like a broken record: "It's not if but when!" and "Legacy signature based solutions are inadequate!" Both of which are true by the way. "It's China!" and "No it's [enter other suspected bad guy here]!" I'm not sure it really matters.

Here's what I consider to be the most important things to think about in light of the latest OPM attack:



- **Security requires a "continuous" mentality.** Attacks are continuous not episodic. The OPM experienced a breach in March of 2014 and a year later it's dealing with another breach. Sally Beauty Supply was breached in 2014 and recently experienced another breach. Get the picture?

- **Continuous monitoring is critical.** Continuous attacks require continuous monitoring. Frankly, I think continuous monitoring is widely accepted at this point with many organizations investing significant dollars in detection solutions, SIEMs, etc. It's essential, but it isn't enough.

- **Deploying more contemporary security solutions can help.** It's become clear that in order to gain increased visibility into environments and detect today's threats organizations need to deploy more contemporary detection solutions and security analytics capabilities. In the case of OPM, following its March 2014 breach it undertook "an aggressive effort to update its cybersecurity posture adding numerous tools and capabilities to its networks." With respect to the

recent breach, a DHS official indicated that the "good news" was that the OPM discovered the breach using the new tools. This is a real world example demonstrating the benefits of deploying new tools.

- **Invest more in response and shift the mindset to continuous response.** If attacks are continuous and we are continuously monitoring, then the next logical step is to adopt a continuous approach to response. I think the first step in this journey is for organizations to invest more in response, period. People, process, and technology are all important. The response mindset also needs to change. Historically, response has been episodic or event-driven ("I've been attacked – Do something!) This mindset needs to shift to continuous response ("I'm getting attacked all the time – Do something!"). A key ingredient to enable continuous incident response will be the increasing use of automation. Why? Automation is required to keep up with attackers that are leveraging automation to attack. It's also required to address a key challenge that large and small companies face – the significant cybersecurity skills shortage.

Attacks like the one on OPM aren't going away. We need to learn what we can to reinforce our defenses. The answer lies in finding ways to continuously detect, investigate and remove advanced threats within the network before attackers can steal data, compromise intellectual property or cause process disruption.

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 COMMERCIAL UAV SHOW ASIA 2015

30 June – 1 July 2015,
Suntec Convention Centre,
Singapore

The first & only business platform in Asia for the buyers & sellers of commercial UAVs/drones

Regulators and more than 50 industry leaders will be presenting their successful case studies & experiences in applying unmanned technologies. Hear from the likes of BP, UVS International, ICAO, EASA and more. This event is a must attend for anyone looking to make connections in the Asian unmanned systems market.

FEATURED SPEAKERS

Claus Nehmzow,
Digital Innovation Organization,
BP, Singapore

Peter Van Blyenburgh,
President,
UVS International, France

Leslie Cary,
RPAS Program Manager,
International Civil Aviation Organisation (ICAO) Panel Secretary, Canada

SPONSORS & EXHIBITORS

BRONZE SPONSORS:

Advanced Innovative Engineering · Aero-Persistence Research · Airware · ALTADEVICES · delair-tech · EuroUSC · IH · Imagemaps · Leica Geosystems · senseFly · ST Aerospace · UAVOS · YUNEEC

EXHIBITORS:

INSIGHT ROBOTICS · ITCHIMI.ASIA Unmanned Aerial Systems · service-drone.com · STERLING COMMS INT'L PTE LTD

QUOTE ADM1 to save $560 off the final price
Book now at **www.terrapinn.com/uav15**

waratek

Waratek Application Security for Java

"The INFOSEC Leader of 2015" - CDM

www.cyberdefensemagazine.com

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?

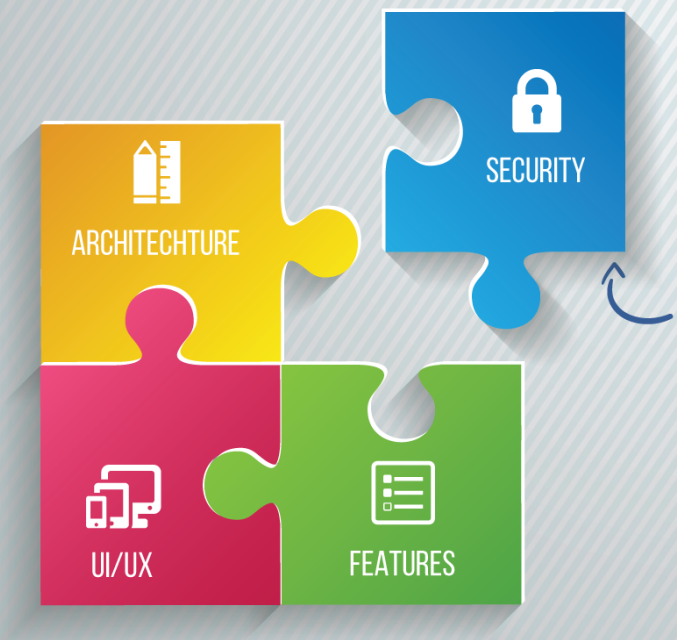
Your Enrollment includes :

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY



You have built a great app with an amazing team.

Let us help you secure it.

SnoopWall's patents-pending AppShield™ SDK can secure any mobile app on all major platforms. Our AppShield SDK makes your app invisible to any other app on the mobile device which might otherwise eavesdrop on it, just like the B2 Bomber employs stealth technology to evade radar detection. With 24/7/365 active monitoring, regular updates and a dedicated team of cybersecurity experts, you can be assured that your app's security and customer data are safe, all the while providing a non-intrustive customer experience.

KEY FEATURES

- Cloaking Technology (patents-pending)
- Dynamic Port Management (patents-pending)
- No Need for Code Obfuscation
- No Malware Scanning Required
- No Backend Database Required
- Root & Jailbreak Detection
- Secure Storage for Data Hiding
- Application Hardening Technology
- No Known Way to Exploit
- Detects & Blocks Tomorrow's Threats
- Apple iOS, Google Android, Microsoft Windows
- No Sysadmin, no Reboot, no special Privileges
- Tiny Deployment Size & Rapid Integration
- Most Cost Effective Per Deployment Pricing

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

Does your mobile app have built-in next generation firewall technology to safeguard customer data?

Mobile apps are critical and vulnerable touchpoints in most companies networks. Just like the firewall which protects your IT network, an app firewall is needed to protect your mobile app. However, most app development teams do not have this expertise, nor are they dedicated to this mission.

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

- HIGH RISK OF PATENT INFRINGEMENT $$$$$
- MAJOR DISTRACTION FROM CORE DEVELOPMENT FOCUS
- HIGH REPUTATIONAL RISKS
- POSSIBLY NOT SECURE
- UPDATED WHEN YOU CAN FIND THE TIME
- FULL BLOWN SOLUTION WILL TAKE YOU 20,000 CODER HOURS (10 CODERS FOR 12 MONTHS)
- LIGHTWEIGHT RISKY SOLUTION WILL TAKE YOU 10,000 CODER HOURS (10 CODERS FOR 6 MONTHS)
- MAINTENANCE AND SUPPORT WILL TAKE YOU 5200 HOURS PER YEAR (2 CODERS FOR 12 MONTHS)
- HIGH RISK TO BREAK YOUR AWESOME APP AND USER EXPERIENCE
- HIGH RISK TO CAUSE USER CONFUSION AND LOSS OF CUSTOMERS
- MAY LOSE SOME OR ALL CUSTOMER RECORDS
- MAYBE SSL PINNING IS THE MOST YOU CAN DELIVER
- MAY PROTECT SOME OF THE PORTS SOME OF THE TIME
- TIME TO DEVELOP AND DEPLOY: 6-12 MONTHS
- **COST TO DO IT YOURSELF: $1.2M**
- **ANNUAL COSTS TO KEEP IT UP TO DATE: $650k**
- **COSTS TO AVOID PATENT INFRINGEMENT: $500k-1.5M**

VS.

LICENSE OUR AppSHIELD SDK

- ✓ PROTECTED ACCESS TO PATENTED AND PATENT PENDING SOLUTIONS
- ✓ LEVERAGE YEARS OF MOBILE SECURITY EXPERTISE
- ✓ LOW REPUTATIONAL RISKS
- ✓ EXTREMELY SECURE AND PROVEN SOLUTION
- ✓ 7x24x365 CYBERSECURITY PROTECTION
- ✓ THE SOLUTION IS DONE
- ✓ THE SOLUTION HAS BEEN PROTECTING MILLIONS OF TRANSACTIONS SINCE 2014
- ✓ MAINTENANCE AND SUPPORT IS INCLUDED
- ✓ INCLUDED IN THIS SYSTEM:
  - → ZERO DAY MALWARE PROTECTION
  - → ADVANCED PERSISTENT THREAT PROTECTION
  - → FEATURES INVISIBLE TO CONSUMER EXPERIENCE
  - → ALL MOBILE APP CUSTOMER PII PROTECTED
  - → MILITARY GRADE ENCRYPTION
  - → REAL-TIME DATA LEAKAGE PROTECTION
- ✓ **TIME TO INTEGRATE AND DEPLOY: 3-5 BUSINESS DAYS**
- ✓ **NO INFRINGEMENT RISKS ONCE LICENSED: FIRST OF ITS KIND IP**
- ✓ **ANNUAL UPDATE COSTS A FRACTION OF DO IT YOURSELF**
- ✓ **PRICING IS A NO-BRAINER (MUCH MUCH LOWER)**

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

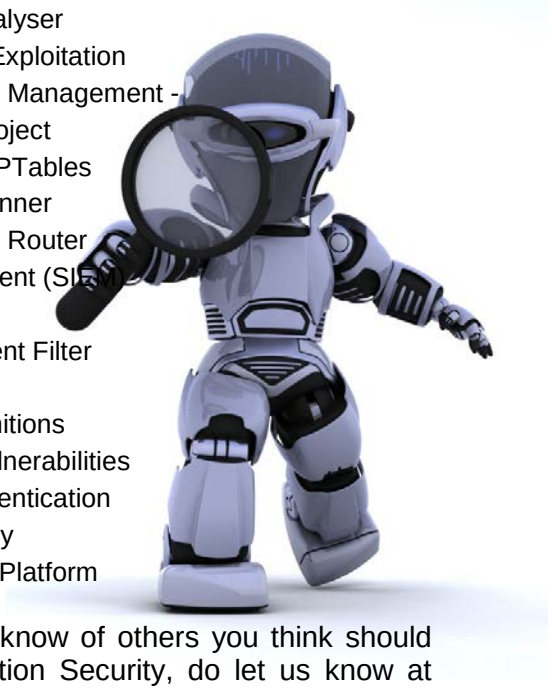
Top Twenty INFOSEC Open Sources

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

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

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available (Version 6 & earlier)
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.

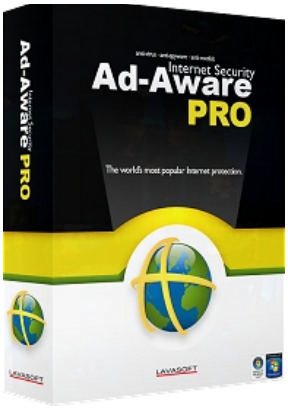
So use it by going here:

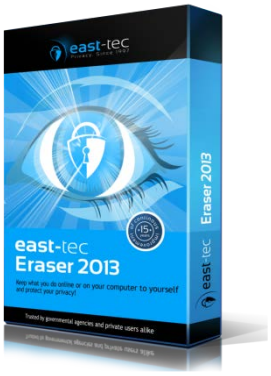
http://www.naisg.org/techtips.asp

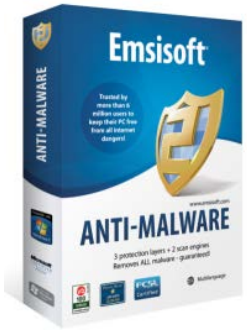
SOURCES: CDM and NAISG.ORG

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 June 2015

Sample Sponsors:

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

Cyber Warnings Newsflash for June 2015

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Here is a summary of this month's cyber security news. Get ready to read on and click the links below the titles to read the full stories. So find those of interest to you and read on through your favorite web browser…

Director of National Intelligence blames China for OPM hack

http://www.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/

Theft of Saudi documents suggests an Iranian hack

http://www.washingtonpost.com/world/middle_east/theft-of-saudi-documents-suggests-an-iranian-hack-experts-say/2015/06/25/dd2f57e2-19c2-11e5-bed8-1093ee58dad0_story.html

Sony Neglect Of "Basic Safeguards" Enabled Hack Attack: Fortune

http://deadline.com/2015/06/sony-hack-attack-safeguards-interview-fortune-1201455482/

Hack of Federal Employee Info Has Comstock Looking for Answers (ICYMI)

http://patch.com/virginia/ashburn/hack-federal-employee-info-has-comstock-looking-answers-icymi-0

U.S. government hacking number sparks unusual drama at Senate briefing

http://www.cnn.com/2015/06/24/politics/opm-hacking-senate-briefing/

What the Houston Astros hack can teach you about cybersecurity

http://www.cbsnews.com/news/what-the-houston-astros-hack-can-teach-you-about-cybersecurity/

OPM inspector general questioned over hacking report

http://www.cnn.com/2015/06/16/politics/opm-hack-ig-testimony/

Spy expert sees more 'Hack-gates' taking place in the years to come

http://espn.go.com/blog/sweetspot/post/_/id/59505/spy-expert-sees-more-hack-gates-taking-place-in-the-years-to-come

F.B.I. Struggles to Pinpoint the Fingers Behind a Hacking

http://www.nytimes.com/2015/06/23/sports/baseball/in-baseball-hacking-case-blunder-helps-fbi-solve-one-riddle-where-but-not-another-who.html?_r=0

China's Hack Just Wrecked American Espionage

http://www.thedailybeast.com/articles/2015/06/15/china-s-hack-just-wrecked-american-espionage.html

Irony alert: Password-storing company is hacked

http://money.cnn.com/2015/06/15/technology/lastpass-password-hack/

Polish LOT aeroplanes grounded by computer hack

http://www.bbc.com/news/world-europe-33219276

CONFIRMED: Chinese government hackers linked to historic hack of US security clearance info

http://www.businessinsider.com/confirmed-chinese-government-hackers-linked-to-historic-hack-of-us-security-clearance-info-2015-6

Samsung Galaxy phone hack: SwiftKey vulnerability lets hackers easily take control of devices

http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsung-galaxy-hack-swiftkey-vulnerability-lets-hackers-easily-snoop-on-phones-10325574.html

Attackers Stole Certificate From Foxconn to Hack Kaspersky With Duqu 2.0

http://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/

FBI seized tech from home linked to celebrity hack

http://www.cnn.com/2015/06/10/politics/celebrity-hack-search-warrant-emilio-hernandez/

Syrian Electronic Army Claims Hack of Army Website

http://www.nationaljournal.com/tech/syrian-electronic-army-claims-hack-of-army-website-20150608

None of us is safe: Major cybersecurity company hacked

http://www.cnet.com/news/none-of-us-are-safe-major-cybersecurity-company-hacked/

U.S. Power Grid Being Hit With 'Increasing' Hacking Attacks, Government Warns

http://freebeacon.com/national-security/u-s-power-grid-being-hit-with-increasing-hacking-attacks-government-warns/

Banking malware proves tough to repel

http://www.pcworld.com/article/2941692/banking-malware-proves-tough-to-repel.html

Study: Click-fraud malware often leads to more dire infections

http://www.scmagazine.com/damballa-issues-state-of-infections-report-on-click-fraud-and-ransomare/article/423167/

Top 10 most read: Dyre malware, Google email undo and UK tops mobile speed charts

http://www.v3.co.uk/v3-uk/news/2415272/top-10-most-read-dyre-malware-google-email-undo-and-uk-tops-mobile-speed-charts

Zeus and SpyEye banking malware gang arrested in Ukraine

http://www.computerworlduk.com/news/security/zeus-spyeye-banking-malware-gang-arrested-in-ukraine-3617939/

Rombertik: what you should know about the evolution of destructive malware

http://www.scmagazineuk.com/rombertik-what-you-should-know-about-the-evolution-of-destructive-malware/article/423272/

Of Ma And Malware: Inside China's iPhone Jailbreaking Industrial Complex

http://www.forbes.com/sites/thomasbrewster/2015/06/26/china-iphone-jailbreak-industry/

Tinba malware that can update itself uncovered by Malwarebytes

http://www.theinquirer.net/inquirer/news/2414993/tinba-malware-that-can-update-itself-uncovered-by-malwarebytes

Stealthy Fobber Malware Takes Anti-Analysis To New Heights

http://www.darkreading.com/vulnerabilities---threats/stealthy-fobber-malware-takes-anti-analysis-to-new-heights/d/d-id/1321055

'Blackshades' Malware Co-Creator Sentenced to Five Years in Prison

http://www.newsweek.com/blackshades-malware-co-creator-sentenced-five-years-prison-346634

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

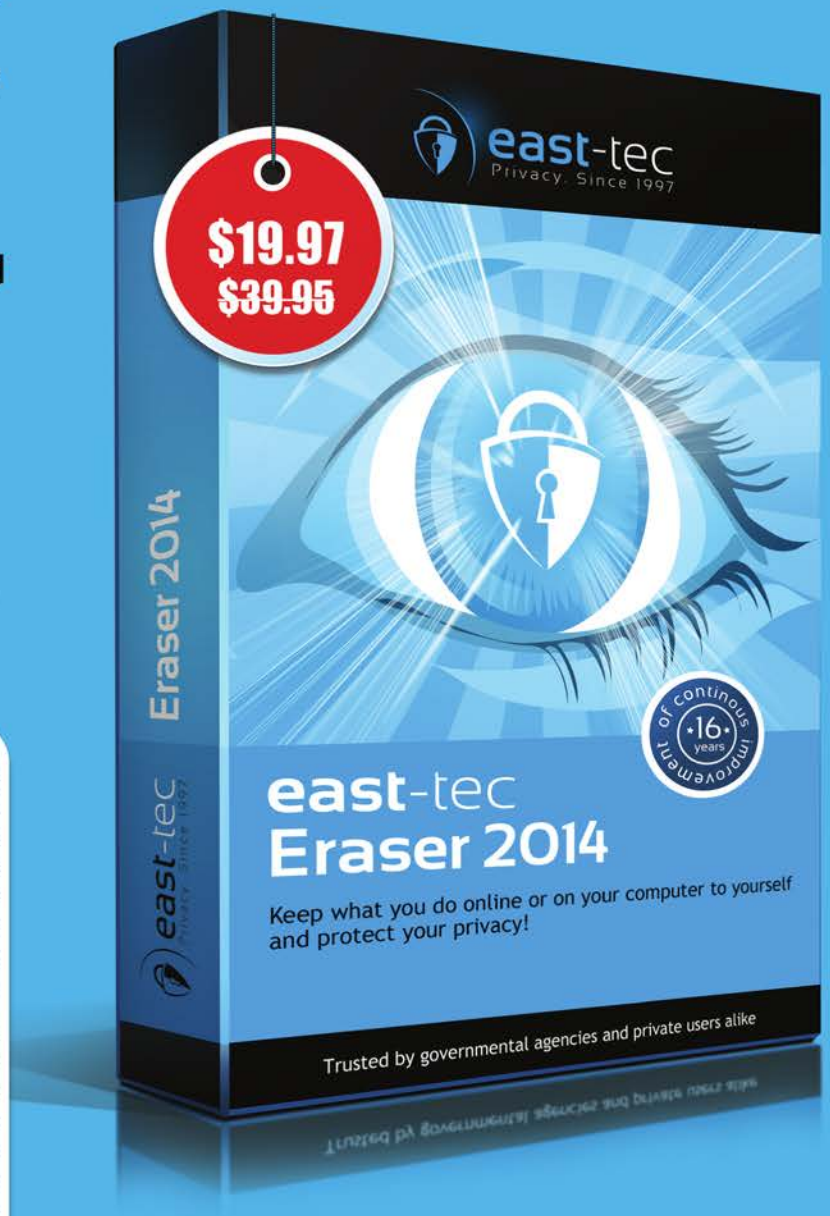
Cyber Defense Magazine - Cyber Warnings rev. date: 06/30/2015

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