CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Threat Intelligence
Cyber Tracking
Social Engineering
Cloud Security

MAY 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

Jim Anderson
Haim Koschitzky
Nahim Fazal
Todd Weller
Bill Mann
Steve Morgan
Ric Jones
Nick Rojas
Milica Djekic
Luis Betancourt
Brian Beyer
Michael Buratowski
Mike Sconzo
Scott Aken
Joe Ferrara
Mark Bevilacqua
Jeff Hussey
Kyle F. Kennedy

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Eye opening innovations from RSA Conference 2015

Friends,

What a wonderful time our team had at the RSA Conference 2015. We sent our executive producer, two reporters and had the pleasure of having one author on assignment also attend on behalf of CDM.

This year was, by far, the biggest RSA conference ever. More exhibitors, more speakers and more attendees. It seems that we also face the biggest reason, today - more breaches.

As you read on, you'll see why we predicted at RSA that many breaches will be on health care (because of the value of a 'fullz' - ie a full PII data theft on an individual), retail and banking this year.

Most importantly, expect the new target vector to be your mobile devices so on a consumer side, there's serious mcommerce and mbanking risk and on a business-side, the BYOD dilemma.

It's also time for CFO's to get into the mix and support the budget needs of their CIO and CISO counterparts, so that the IT staff can fend off the next breach and ensure regulatory compliance without issues that could impact the bottom line.

This is an information packed edition of Cyber Warnings so we hope you enjoy reading it and sharing it with your friends.

Check out our RSA Conference 2015 Trip Report on page 74 for the latest innovations in cyber security.

To our faithful readers, Enjoy

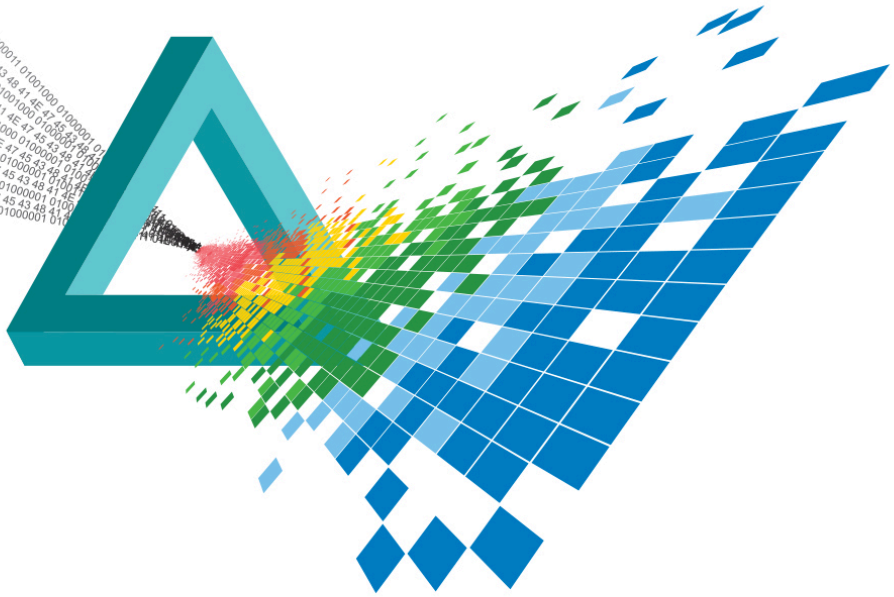
Pierluigi Paganini

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

RSA Conference Unveils Unique Challenges and Trends as Cyber Attacks Mature

By Jim Anderson, President of the Americas for BAE Systems Applied Intelligence

RSA remains the premier gathering for industry experts across a wide array of cyber security, threat intelligence and breach remediation. The 2015 conference was no different and served to highlight many of the unique challenges that IT professionals face in a technologically advanced society. For those in the field, RSA highlighted three important trends practitioners should know about: security has escalated from an IT risk to a board room issue, cyber crime "detection" has become more important than "prevention" and criminals are far more organized than ever before.

Security is now a board room issue - While the role of IT has typically been the purveyor of all things security, across the industry, RSA saw a heavy focus on elevating the risk of our hyper-connected world to the board room. At RSA, it was apparent that boards became more sensitized to the "business risk" associated with being a victim of cyber crime. As a result, their concerns have evolved, and many boards are now wondering if what happened to Sony can happen to them.

What this means is that if a board hasn't yet asked for updates regarding its exposure to crime, it will soon. Therefore, Chief Information Security Officers (CISOs) and other IT executives must now be prepared to discuss the complex realities of cyber crime with a much broader audience and make recommendations on selecting the proper approach to both augment security around the network and mitigate damage. This means a new level of communication among the board, CISOs and the IT team is mostly about education and expectation setting. The board must learn more about the security space, but equally so, it's imperative for IT teams to convey business risk in terms the board can use to guide decisions.

Security is about connecting the dots… faster - Attackers have gotten agile, making it nearly impossible for organizations to keep pace. For years, digital security was about building the strongest firewall and defense system available. Today, that approach simply won't work.

In the US, according to Identity Theft Research Center (ITRC), nearly 800 companies suffered a data breach last year. IT teams must now act as though attackers have made it beyond their perimeters and into their networks. IT teams should implement a variety of technologies that can help to quickly identify behavioral oddities that would be associated with an intruder. These solutions should include big data technologies and predictive analytics that can shorten the time period from "breach" to "discovery" and prevent criminals from leaving with assets.

At the same time, as the scale of the threat continues to grow exponentially, companies are turning to providers of managed services to deal with the shortage of cyber analysts. These external resources can also incorporate aggregated data from across their client base to improve security for each company they protect.

Disorganized cyber crime doesn't exist - Organized criminal enterprises are an advanced, persistent and very real threat. They are supported by integrated criminal supply chains, are highly creative and exploit the fact that their victims' networks are far flung and porous.

According to reports from RAND, the world of hacking has become more organized and reliable in the last 15 years and 80% of hackers work with organized crime groups. Today, known security flaws spread like wildfire, as criminals gain insights on the most effective attack methods from each other.

IT professionals and teams that are able to effectively communicate risk with leaders in an organization will be better positioned to mitigate those risks. This means stronger preparation against advanced threats and quicker mitigation once a thief has breached a company's security. It also means revisiting known flaws. A report from Verizon shows that a significant majority of successful hacking efforts were perpetrated using vulnerabilities that have been around since 2002.

Deflecting cyber criminals is no easy task. Organizations must have successful collaboration among their Board of Directors, CISOs and their IT teams. They must respond expeditiously to known vulnerabilities, and assess that they have the proper resources to agilely address a cyber attack. They must effectively plan to mitigate damage in the event of a hack. Companies that are able to incorporate these initiatives will ultimately be the winners against cyber crime.

About the Author

Jim Anderson, President of the Americas region, BAE Systems Applied Intelligence, brings over 25 years of experience of sales and consulting with organizations in the high tech industry. Most recently, he served as Global Sales Director, Unified Computing at Cisco, Inc. Prior to that, Jim was with Dell, Inc. where he served as VP, Server and Storage Sales for the Public Sector. Before his tenure at Dell, he served in various leadership roles at Hewlett-Packard for 14 years. Anderson holds a bachelor of science in electrical engineering and computer science from Princeton University and an MBA with a concentration in marketing from the Wharton School, University of Pennsylvania, Philadelphia, PA.

XpoLog – Turning Data into Action

XpoLog, a privately held software company, has created a tool that understands data, unlocks its hidden value, and helps you find, troubleshoot, report, and visualize mission critical information whether in your local storage, or in the cloud. Unlike others, XpoLog provides an automatic Analytic Search that layers automated intelligence in the context of user searches. Analytic Search proactively scans log data and correlates analytics layers. You can leverage the technology in IT Operations, DevOps, APM, Software development, Software testing, and Security Log management.

This unique technology, and specifically the Analytical Search engine, is designed to effectively deal with **any** log or machine data, even custom applications such as **home-grown applications**.

Last month, XpoLog was included in the list of "Cool Vendors" in Gartner's "Cool Vendors in IT Operations Analytics, 2015" report by Will Capelli and Colin Fletcher. Gartner Inc. is a world leading IT technology research and advisory company. Vendors selected for the Gartner "Cool Vendor" report are known to be innovative, impactful and intriguing.

"We are very happy to be included in the Cool Vendor report by Gartner, and we consider this yet another confirmation that our focus on advanced analytics and search for IT data will help our customers turn silos of unstructured data into meaningful intelligence and actions" said Haim Koschitzky, CEO of XpoLog. "With the upcoming launch of our latest version, XpoLog 6, we believe our product will revolutionize the speed and analysis of big IT data."

XpoLog is currently in the midst of releasing its latest upgrade, version 6. **XpoLog 6** focuses on creating a context of virtual application structures that enable applications and operation groups to organize data in the context of business services. By virtualizing the data sources in logical application structures, various groups can build advanced analytics and seamlessly move back and forth between pre-production and production. In order to support the growing demand for data visualization, XpoLog has added more than 20 new visual components and new ways to present data in a continuous fashion.

"In recent years, as we focused on building more value for our customers and partners, we recognized a problem with manual data analysis solutions, especially with home grown technology and cloud deployments. By adding new technology that layers analytic insights in the context of data analysis, we help extract meaningful intelligence from log data on an entirely new level of efficiency and accuracy" said Haim Koschitzky, XpoLog CEO.

The XpoLog 6 primary enhancements are:

- Virtual application structures and data sources
- New Operations/DevOps/NOC/SOC rooms view with themes and animated slide-shows
-

- New AngularJS Single Page app UI/UX
- More than 20+ new visualization gadgets including 3D types
- Optimized Analytic Search with more Analytic Layers

“We recognize that advanced analytics and more powerful visualization tools for log data are major requirements for log management solutions. We see organizations adding XpoLog Analytic Search on top of existing log management deployment, such as open source platforms, in order to extract more value from their IT” says Gal Berg, XpoLog VP of Engineering.

One of the many new features of XpoLog 6, is the **Ops View**. Different Operational groups require different tools, and also different views. Sometimes the same operational group may require different views for different situations.

The teams at the NOC, Operations, DevOps, SOC or High availability control rooms need to have ongoing status screens of managed environment. The need for an ongoing streaming of status views is very different from a single dashboard view or a search console. With XpoLog 6 you can select multiple dashboards and run them as slideshows. You can build visual dashboards for security, performance, errors, business statistics, and any other view you need.

You can also build Availability and Business slideshow Views for application and business owners. Build R&D, Development, and Testing dashboards and let them slide in the meeting rooms. Operations, Security, and DevOps will be able to build multiple dashboards and Apps that will provide continuous feedback on systems and applications.

You can even select a “night mode” theme in the dashboard view that will invert the colors of the visualization views. This is useful for those NOC technicians monitoring in dark control rooms. After all, red shift does not have to mean red eyes…

About the Author

Haim Koschitzky is the founder and CEO of XpoLog. He has spent the past decade and a half developing his software which combines human intellect and advanced machine analytics algorithms from vast amounts of log data. He has his degree in Computer Science from the Interdisciplinary Center in Herzliya, Israel, and was also a developer at Mercury Interactive, later bought up by HP Software.

Are Your Files Protected From The Cloud?

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

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

Visit GoAnywhere.com for a free trial.

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

GoAnywhere.com 800.949.4696

SAVES US A LOT OF TIME AND HEADACHE

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

Matt Booher
President
WIS:DOM Information Systems

Threat Intelligence & RSA

RSA 2015 was very much the year of Threat Intelligence. That is the overwhelming sensation one is left with as the dust settles on the RSA conference for this year. Perhaps more than any other expression Threat Intelligence (TI) was the one that everyone seems to have adopted and made their own this year. I was trying to count the number of times I saw that phrase as I walked down the exhibition halls and I gave up after 3 minutes. I think by that that time I had seen the phrase at least on 15 booths.

I was surprised that even traditional SIEM vendors had adopted this term in an attempt to define their own solutions. But what this perhaps reflects is that end users have an increasing urgency and need for TI.

Listening to the many people that came to speak to Blueliv it was clear there is a need for TI but end users are not quite sure how to deploy and use TI. I was also struck by the fact that the words APT seemed to have faded somewhat into the background noise of the conference. This was the buzzword of last year and this year there seems to have been a significant shift towards trying to grapple with and understand how best to deploy and use TI.

Integration was the second theme that struck me has coming to the foreground this year. There were many people that spoke to me about their frustration as to how the tools that are supposed to identify security compromises more often than not fail to do so. What could be done to try and improve existing security real estate that has already been deployed?

There is no appetite to rip out expensively installed hardware, what there was however was a desire to feed threat intelligence into these devices to make them smarter. So what I heard from the many that visited the Blueliv booth was can TI be integrated with what I have already deployed? From the Blueliv perspective the answer was a resounding “yes it can”.

Finally, from a personal perspective, what for me was the most enjoyable part of the conference was the diverse range of organizations that were present there. I think I just about spoke to everyone from all of the continents around the world! Or is that my mind playing tricks on me? It felt that way!

The conference was a wonderful opportunity to reach out and share our passion about security with people face to face that you would never otherwise have an opportunity to engage with.

Everyone was speaking the language of security and everyone was asking the same question: how can we become more effective in dealing with the threats that are emerging and how can we move to a more strategic approach in dealing with cyber security threats and risks.

www.blueliv.com

About the Author

NAHIM FAZAL, Head of International Business Development, Blueliv

Nahim Fazal heads up cyber security international business development at Blueliv. During the last eight years, he has successfully developed and delivered innovative cyber threat and fraud solutions. He is responsible for aligning the Blueliv strategy with the unique needs of a broad range of industry verticals including financial services, utilities and service providers across the globe. Nahim leads engagements with C-Level clients, partners and analysts. He is also responsible for building and driving forward relationships with governments and global law enforcement agencies. Nahim honed his cyber risk management skills in multinational financial services organizations including global banking institutions such as RBS and HBOS, and the cyber security firm S21sec. He is also a respected speaker and thought leader on issues relating to cyber security. Nahim was the founding director of the European Cyber Security Group and has provided cyber intelligence briefings within the Financial Crime Prevention community, law enforcement agencies, (EUROPOL, INTERPOL) and public sector organizations. Nahim studied Law at De Montfort University (United Kingdom), where he earned his LLB (Hons).

About Blueliv

Blueliv is a leading provider of targeted cyber threat information and analysis intelligence for large enterprises, service providers, and security vendors. The company's deep expertise, data sources, and big data analysis capabilities enable the clients to protect against cyber attacks. Its turnkey cloud-based platform addresses a comprehensive range of cyber threats to turn global threat data into real-time actionable intelligence specifically for each client. Blueliv's clients include leading bank, insurance, telecom, utility, and retail enterprises in Europe, and the company has alliances with leading security vendors and other organizations to share cyber intelligence.

Hackers Using Macro-Based Malware to Breach Business Networks

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

Trends and fads move in cycles - things that were once popular fade into obscurity and later, may make a roaring comeback. Synth-heavy pop music, 1970s-style jumpsuits and facial hair on men are all in fashion again today, after spending considerable time as relics of a time gone by. Unfortunately, the same forces are at play in the world of cybercrime, as hackers bring back the once-popular macro-based malware.

According to a blog post from Microsoft, the number of reported malware incidents plummeted after the company made "Disable all macros" the default setting on its Microsoft Office software. But the macro is making a comeback today, thanks to new forms of social engineering and phishing emails.

Malicious macros are back and more convincing than ever

Microsoft explained that the disabled-by-default macros in its products are no longer sufficient to protect users from malware. The problem is that hackers have made their phishing emails so convincing that they can actually trick users into manually enabling the macros in their Office suites.

Two of the most popular resurgent Trojans that hackers are using are called Adnel and Tarbir. These are being spread through spam email campaigns that target both home and enterprise users all over the world, though the infections seem to be more concentrated in the U.S. and U.K.

Security researchers at Microsoft found that both types of malware are being embedded within phishing emails with titles like "Invoice as requested," or "Payment Details." Attached to the emails are Word documents claiming to have information for the reader, and the emails

even have detailed steps to help users enable macros. Once the user opens the document, the macro triggers the infection and allows malware into the system.

Employee training isn't enough to prevent malware infections

In the past, phishing emails were often comically amateur, written in broken English that most people would recognize as being a scam (Nigerian prince emails come to mind). But today, these emails are incredibly convincing, with very real-looking serial numbers and even barcodes. The average employee with a rudimentary knowledge of cybersecurity is highly unlikely to be able to spot a malicious email, no matter how well-trained he or she is.

Enterprise security teams need to recognize that there's no way to prevent every single employee from opening every suspicious email that comes his or her way. Advanced security tools can cover them where employee training can't by providing an active defense grid that continuously monitors the endpoints and the network for threats and automatically neutralizes them as they appear. Given how easy it is for malware to make it past the perimeter, security teams need a way to get a forensic look inside their networks and protect the valuable data within.

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.

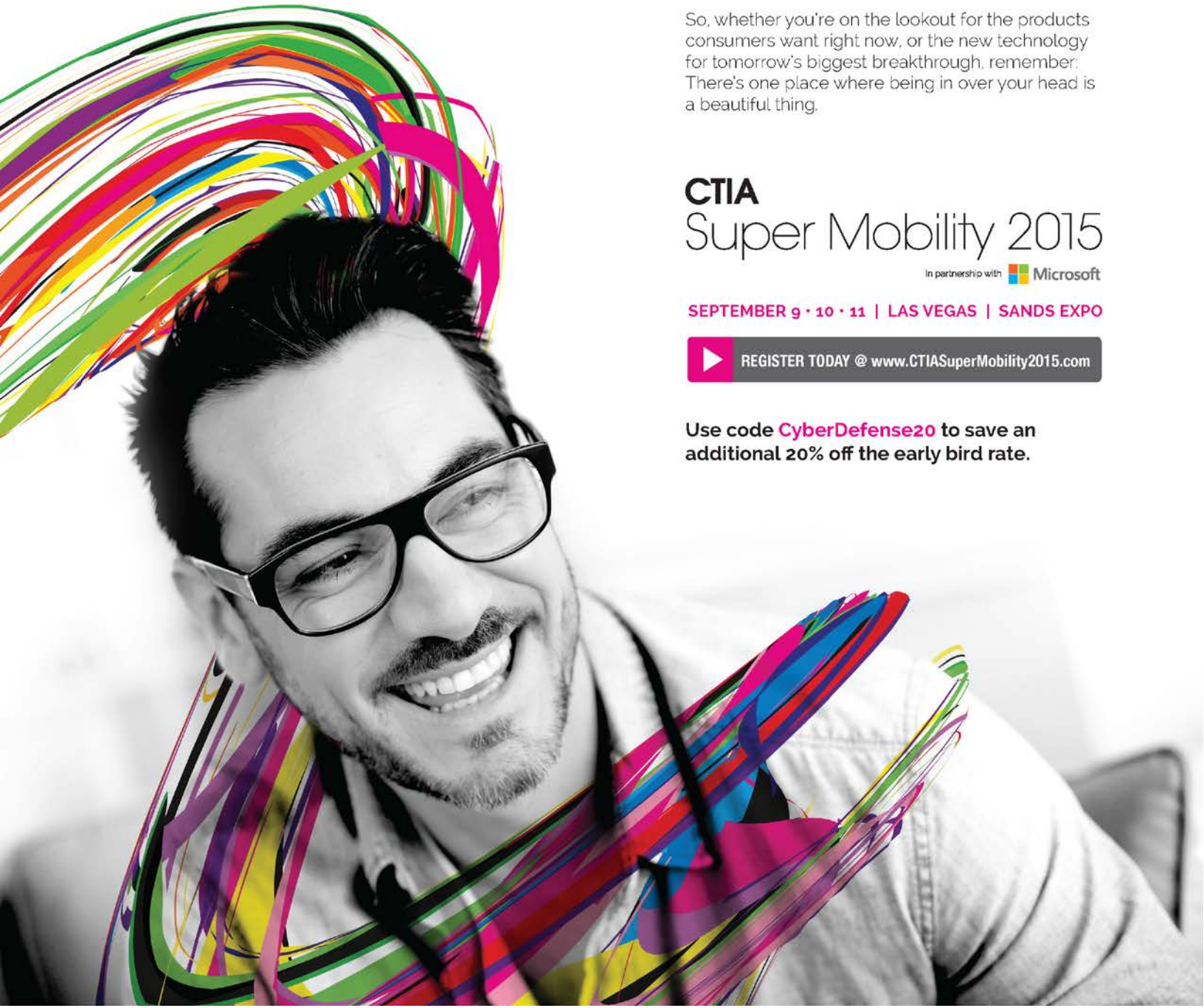
CTIA
Super Mobility 2015

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.



Has Your IT Been Left in the Dark?

By Bill Mann, Chief Product Officer, Centrify

According to research[1] by Elastica, most companies today are using over 500 cloud applications, and while the applications themselves may seem to be secure, employees are increasingly using them without IT's knowledge or involvement – opening up potential security risks and often violating corporate regulations.

This use of unauthorized cloud applications, known as Shadow IT, presents something of a dilemma for businesses. On the one hand, it presents an easy solution for departments looking to make cost savings with zero infrastructure requirements, and avoids the time needed to make a request to IT, which then has to approve and procure the software.

On the other hand, using these applications can pose a variety of security risks. Allowing them to be used indiscriminately without putting the right security controls in place could lead to a security breach, putting everyone at risk.

It is easy (and tempting) however, for staff to circumvent corporate IT policies by introducing these applications, speeding up the process of acquiring what they feel they need to do their job. If IT denies access to such applications, they are seen as impeding productivity.

A recent report by CipherCloud revealed that enterprises vastly underestimate the extent of Shadow IT within their organizations.

The statistics highlighted that on average 86 percent of cloud applications are unsanctioned.

A poll at Cloud Expo in London this year by Centrify showed that over two-thirds of organizations admit cloud applications implemented without IT's knowledge or involvement pose a security risk to the business.

While just half of respondents were confident that less than 10 percent of applications were implemented in this way, it supports the theory that the extent of the problem is being hugely underestimated.

Just a few years ago such things would have been unthinkable, with applications tightly controlled and procured through the IT department.

But with the consumerization of IT – driven by the proliferation of mobile devices and prevalence of cloud applications – our behavior has changed, despite the growing number of security threats and daily headlines about serious breaches.

[1] http://www.centrify.com/resources/4277-top-7-ways-to-protect-your-data-in-the-face-o

Clouding your Judgement

The nature of Shadow IT creates a void, with IT departments left in the dark when it comes to who is accessing what, where and when. In the past, IT managed the identities for any resources used by employees relatively easily because resources and users sat within the corporate firewall. Today, these same users and resources may be outside the data center, either in an authorized application deployed by IT, or, as we've identified, by departments within the business deploying and using their own unmanaged (and unsecured) applications.

With identities now residing outside the corporate firewall and on disparate systems, and no means of control over applications and the data they hold, organizations need to reconsider their identity and access management (IAM) infrastructure.

Employees tend to be careless with their identities – the old sticky notes stuck on PCs in the office are still in evidence – and many do not appreciate the damage that bad password hygiene can cause.

The likelihood is that most people re-use the same passwords across multiple apps, sites and services, or use weak memorable passwords, which can expose organisations to attack if their details are compromised.

In a survey we conducted last year among 1,000 U.S. workers, we found that over a third of us now enter more than 4,000 passwords online per year, wasting about 24 hours annually in the process. It's no wonder we are tempted to use the same password time and time again or ones that we can easily remember!

Then there's the challenge of managing user access rights for these unauthorized apps once an employee leaves an organization. If the IT department is not privy to all of the applications a person had access to during their time at the company, and the log-in details of a given application, removing access becomes increasingly difficult as it falls outside the realm of corporate IT.

Users must be encouraged to ensure authentication is secure. The best way to do this is to extend existing corporate IT password policies and procedures, leveraging a user's corporate identity to authenticate to applications wherever they may be, and from whatever device they are using – whether on-premises or remotely. This should also be backed up with multi-factor authentication, such as the user acknowledging via their mobile phone that it is actually them trying to access an application.

By incorporating Identity as a Service (IDaaS) and single sign-on (SSO) for all cloud applications, organizations can eliminate the security concerns of password re-use and enable provisioning and deprovisioning of users based on their role as defined in a centralized directory service, like Microsoft Active Directory.

Being able to automatically provision and deprovision accounts is critical for controlling application security, especially as employees are hired, change job titles, move between groups and eventually leave the company.

Finally, organizations need to look at the mobile devices being used by employees. In the age of BYOD, employees want to use their own smartphones and tablets to access work resources. At the very least, they should have some kind of passcode, and it's surprising how many people do not use them today.

Our survey last year revealed that while around half the respondents use their personal mobile devices for work, nearly 40 percent say they do not use passcodes on them even though they have access to email, confidential documents, customer contact data and even budget information.

With the right solution, IT departments can manage in-built mobile device features, such as Samsung KNOX or managed applications within iOS 8, to enable the separation of work and personal applications. This allows them to control what is being used and by whom to create a much safer environment for running apps.

Rapid growth in the use of cloud applications, authorized or not, presents new challenges for corporate IT. The responsibility ultimately lies with the IT department to secure them and to provide the proper access control and authority to use them. This requires organizations to develop security best practices for adopting cloud applications. The process starts with acknowledging Shadow IT as an issue and identifying the cloud applications being used by employees.

By centrally managing user identity and adopting a single sign-on approach, companies can find a balance between productivity and security. By applying security policies to devices and passwords, IT is given the means to maintain security and avoid the risk of a data breach.

About the Author

Bill Mann is chief product officer and senior vice president of products at Centrify, where he is responsible for product strategy, management, innovation and evolution.

41 New England Firms Make the Cybersecurity 500

Steve Morgan is Founder & CEO at Cybersecurity Ventures, and Editor-In-Chief of the Cybersecurity Market Report and the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies.

Menlo Park, Calif., May 4, 2015

Cybersecurity Ventures recently announced the Q2 2015 edition of the Cybersecurity 500, a list of the world's hottest and most innovative cybersecurity companies.

The Mass. and greater New England area, long known as a hotbed for computer technology and software, has an impressive lineup of cybersecurity companies.

There are 41 companies with corporate headquarters in Massachusetts on the Cybersecurity 500. The companies in their listed order, with technology category and city are:

7. RSA (division of EMC), Intelligence Driven Security, Bedford MA

9. Veracode, Application Security Testing, Burlington MA

48. Cryptzone, File & Data Encryption Platform, Waltham MA

53. Akamai Technologies, Secure Cloud & Mobile Computing, Cambridge MA

55. CloudLock, Cloud Information Security, Waltham MA

56. Bradford Networks, Network Security Automation, Boston MA

59. Bit9 + Carbon Black, Endpoint & Server Security Platform, Waltham MA

60. Corero, DDoS Defense & Security Solutions, Hudson MA

65. CounterTack, Real Time Attack Intelligence, Waltham MA

80. Core Security, Predictive Security Intelligence, Boston MA

90. SnoopWall, Mobile Device Security, Nashua NH

94. Arbor Networks, DDoS Attack & Threat Protection, Burlington MA

98. Rapid7, Security Data & Analytics Solution, Boston MA

118. Allegro Software, Embedded Device Security, Boxborough MA

125. Resilient Systems, Incident Response Platform, Cambridge MA

126. Confer, Threat Prevention & Incident Response, Boston MA

130. Vaultive, Cloud Data Encryption, Boston MA

131. VASCO Data Security Authentication & e-Signature Solutions, Marlborough MA

141. Courion, Identity & Access Management, Westborough MA

144. WWPass, Authentication & Access Solutions, Manchester NH

148. Digital Guardian, Enterprise Information Protection, Waltham MA

154. Viewfinity, Threat Detection & Protection, Waltham MA

170. Raytheon Cyber & Homeland Security Services, Waltham MA

186. SilverSky, Security-as-a-Service, Milford CT

191. Threat Stack, Cloud Security Monitoring, Boston MA

206. Pwnie Express, Network Security Risk Assessment, Berlin VT

214. Recorded Future, Real-Time Threat Intelligence, Somerville MA

217. Wave Systems, Software for Hardware-Based Security, Lee MA

244. NetScout, Situational Awareness & Incident Response, Westford MA

246. Forum Systems, Secure Cloud Gateway, Newton MA

229 Onapsis, ERP Cybersecurity Solutions, Boston MA

254. AlgoSec, Security Policy Management, Boston MA

281. General Dynamics, Threat Defense Solutions, Boston MA

289. Mimecast, Microsoft Exchange Email Security, Watertown MA

300. GlobalSign, Identity & Authentication Service Provider, Portsmouth NH

337. Prelert, Machine Learning Anomaly Detection, Framingham MA

361. Sqrrl, Cyber Defense Analytics, Cambridge MA

389. Promisec, Endpoint Security Intelligence, Needham MA

408. Syferlock, Software Based Authentication, Shelton CT

423. VisiTrend, Cybersecurity Analytics, Cambridge MA

484. Apperion, Mobile App Security, Boston MA

485. Imprivata, Security for Healthcare Providers, Lexington MA

Massachusetts leads New England with 35 companies listed. The biggest city is Boston with 10 companies. Next is Waltham with 7. Cambridge has 4.

New Hampshire has 3 companies listed. Connecticut has 2, and Vermont has 1.

A couple of New England Cybersecurity companies have rapidly rising profiles:

Waltham MA based Cryptzone, a provider of dynamic, context-aware network, application and content security solutions, recently unveiled its next-generation product at this year's RSA Conference - the top cybersecurity conference held in San Francisco. "With the proliferation of cyberattacks, organizations are increasingly seeking out trusted partners who can provide them with a layered approach to security to stop attackers at every vulnerable organizational entry point," said Kurt Mueffelmann, President and CEO at Cryptzone. "We are honored to be recognized for efforts to resolve multi-faceted and layered issues that security has presented for today's organizations."

SnoopWall, headquartered in Nashua NH, is the top listed mobile device security company listed on the Cybersecurity 500. SnoopWall is the world's first counterveillance software development company focused on helping consumers and enterprises protect their privacy on all of their computing devices, including smartphones, tablets and laptops, through deep integration with high value mobile applications, smart devices and the Internet of things (IoT). "Mobile-device security will become the top requirement this year for mobile banks, retailers and wallets as they move all their transactions into our space," says Gary Miliefsky, CEO at SnoopWall. "That's why we developed our SDK, to provide protection for their apps against the hundreds of millions of pieces of undetectable malware disguised as free trustworthy apps -- just waiting to steal valuable personally identifiable information in the blink of an eye."

New England's major players continue to make waves in the Cybersecurity space:

Cloud application security company Veracode in Burlington MA is planning to go public in May, according to Fortune. Veracode has raised over $110 million in venture capital funding. Its most recent round was a $40 million Series F infusion last September led by Wellington Management.

Defense contractor Raytheon in Waltham, MA is investing $1.57 billion to create a new cybersecurity company with private-equity firm Vista Equity Partners LLC. The new firm will combine Raytheon Co.'s cyber products unit with Websense Inc. (San Diego, CA), which Raytheon agreed to acquire from Vista.

Akamai Technologies has acquired Xerocole (Boulder, CO), a DNS platform provider.

Venture funding is flowing in to some hot cybersecurity companies in New England:

Sqrrl, based in Cambridge, MA, a provider of big data analytics for identifying and responding to cyber threats, raises $7 million in Series B, led by Rally Ventures, joined by Atlas Venture and Matrix Partners. The company also unveiled new software aimed at detecting and responding to cybersecurity threats. Total funding to date is now $14.2 million.

CloudLock, based in Waltham, MA, a cloud based data security company, raises $6.7 million in a 4th round of funding. Company has previously raised $28 million from Bessemer Venture Partners, Cedar Fund and Ascent Venture Partners.

Rapid7, based in Boston MA, a provider of security analytics software and services, closes $30 million in funding from Bain Capital and Technology Crossover Ventures. Rapid7, whose investors include Bain Capital Ventures and Technology Crossover Ventures, has chosen Morgan Stanley and Barclays to assist with an initial public offering, according to Reuters.

Email security vendor Mimecast, based in Boston MA, whose investors include Insight Venture Partners, Dawn Capital and Index Ventures, has spoken to some investment banks about an IPO later this year but has not hired any firms, according to Reuters.

To see the entire list of 500 companies, go to:

http://www.cybersecurity500.com/

To see the Cybersecurity 500 Q2 2015 press release which explains the selection criteria for companies who made the list, go to:

http://cybersecurityventures.com/cybersecurity-500-q22015/

The worldwide cybersecurity market is defined by market sizing estimates that range from $71 billion in 2014 to $155+ billion by 2019, according to the Cybersecurity Market Report. To read the Report, go to:

http://www.cybersecuritymarketreport.com

Steve Morgan is founder and CEO of Cybersecurity Ventures, a cybersecurity research and market intelligence firm since 1999. Steve is Editor-In-Chief of the Cybersecurity Market Report and the Cybersecurity 500.

infosecurity® EUROPE

• 02-04 June 2015 • Olympia • London •

Intelligent security
Protect. Detect. Respond.
Recover.

You can't put a price on high-quality education

REGISTER for the world's biggest **free** Infosecurity Education Programme!
www.infosecurityeurope.com

CELEBRATING 20 YEARS
02-04 JUNE15
OLYMPIALONDONUK

REGISTER FREE NOW

- Access to the experts and industry leaders
- Learn from inspirational speakers
- Network, share, collaborate and build relationships
- Discover new and innovative security solutions
- Earn CPD and CPE credits by attending the free education programme

Managed by:
infosecurity GROUP

Part of:

Three IT Workplace Issues Preventing CIOs from Sleeping Easy

By Ric Jones

No, the term CIO doesn't stand for "career is over." But you can't blame chief information officers for occasionally feeling, well, *stressed* as they deal with the threat of cybercrime, the Cloud, budgetary restraints, increasing business unit demands and data recovery.

No wonder that 91 percent of those responding to CIO magazine's "State of the CIO" report described their jobs as "more challenging" as they struggle with shifting expectations and responsibilities.

So what, in particular, is keeping CIOs up at night? A recent survey of 276 U.S. CIOs and executive IT professionals commissioned by Sungard Availability Services revealed three workplace issues in particular that trigger insomnia. They are security, downtime and talent acquisition. Let's consider each separately.

Security

Security ranks highest among IT concerns, reflecting the increasing frequency and complexity of cyber attacks. For a growing number of CIOs and their companies, it's not a matter of "if" a data breach occurs, but "when." As a result, 51 percent of CIOs believe budgets for security planning should be the last item to be trimmed.

While cyber criminals worry CIOs, they recognize that internal threats often are the root cause of security disasters. Sixty-two percent of surveyed CIOs cited leaving mobile phones or laptops in vulnerable places as their chief security concern, followed by password sharing (59 percent). Sixty percent say they are enforcing stricter security policies for employees this year.

The bottom line: As much as you try to protect your organization from outside threats with the most advanced technology, users still must be responsible for their own and the company's security; they're the first line of defense, especially against phishing and similar breach attempts. And a 2015 priority: educating users to help them change their behavior and stick with compliance on security best practices.

Downtime

Very simply, downtime damages reputations – and costs money. An IDC study released in February put the average total cost of unplanned application downtime per year at $1.25 billion to $2.5 billion for the Fortune 1000. The average hourly cost of an infrastructure failure is $100,000 per hour. And for a critical app failure, it's $500,000 to $1 million per hour.

This explains why 42 percent of CIOs consider their disaster recovery plans to be vital to their organizations and also should be among the last line items cut from IT budgets.

Why? One, the damage to reputation far outweighs the monetary costs associated with these recovery and continuity services. The reality, however, is that CIOs and CEOs (and others in the C-suite) must recognize the necessity of the services, and CIOs must represent accurately the risks involved if budgets are cut.

Downtime also can hurt a company's ability to generate revenue and expand business in the long-term and, for some enterprises, including those in hospitality, once that time is lost, the revenue can't be made up because prospective guests have booked rooms elsewhere.

Talent acquisition

The acquisition of star talent is often simply overlooked, even though its need continues to be a growing challenge for the tech sector. Thirty-eight percent of CIOs voice concern about acquiring the right talent. Half of them don't believe gaining and retaining talent gets the appropriate attention it deserves.

It's not just about finding candidates but about retaining the right skills, landing someone who fits your culture, and sometimes balancing the need for great talent with cost efficiencies.

One idea that can help: Partner with vendors and outsource talent for some IT needs. Still, it's a balancing act between hiring in-house to support core projects and leveraging outside resources for short-term demand.

Life isn't likely to get any easier for CIOs. Consequently, they must continue to focus relentlessly on their operations and business strategy but be mindful of the changing external challenges and trends. This especially applies to issues that impact their security, their operational availability and the ability to attract and retain strong talent.

Perhaps, this will help them rest a bit easier.

About the Author

Ric Jones is CIO of LifeShare Blood Centers, supplies blood components to more than 100 medical facilities and hospitals throughout Louisiana, East Texas and South Arkansas.

How eCommerce Uses Cyber Defense

For businesses that sell online, cyber defense is obviously a primary concern. By now, most customers know to use strong passwords and to change those passwords frequently. But what are eCommerce businesses doing to get ahead of ever-evolving digital threats? As the systems and strategies of their attackers change, so should the industry's defenses.

Cyber Attack Data Sharing: The NATO Mutual-Defense Model

In 2014, Computer Weekly reported that the North Atlantic Treaty Organization (NATO) was amending its longstanding mutual-defense policy to include cyber attacks. The organizing principle of NATO's mutual-defense arrangement is that when a group or country attacks any one of the 28-nation partnership, the other 27 countries are expected to come to that country's defense.

Image Courtesy of Shutterstock

Now, when a member nation is the target of a digital attack, the rest of the group will likewise rush to its aid with "training, education, exercises, malware intelligence sharing, early warning, and incident response."

This all-for-one defense policy isn't just for global political organizations like NATO — the eCommerce industry can apply the same lessons. Facebook's ThreatExchange program is based on the concept that, since cyberattacks are often launched simultaneously against multiple targets in the same industry, all businesses "share in each other's fate." The cyber attack data-sharing initiative is based on the idea that when more companies share attack data, things will be harder for attackers. This is especially important because the success of so many eCommerce sites, such as Shopify, are directly connected to their presence on Facebook.

DDoS as the Preferred Weapon: When Videos are Truly Viral

In 2014, the eCommerce security world was shaken to its foundation when a B2B site was crippled with a distributed denial of service attack. DDoS attacks are nothing new, but the vehicle used to launch the intrusion is what made this attack stand out. The attackers used a viral video from a popular video-sharing site to exploit a persistent cross-site scripting (XXS)

vulnerability. When people viewed the video, they unwittingly bombarded the site, as their computers had become "DDoS zombies".

The ingenious and devastating plot hit an eCommerce security industry that was already jittery after a report by the security firm Incapsula found a 240 percent increase in traditional DDoS attacks between 2013 and 2014.

The video-sharing attack proved that DDoS is the tool of choice for cybercriminals, and as their strategies are becoming more sophisticated and unpredictable, the primary focus of the eCommerce security industry is to regain ground lost in this area to cyber criminals.

eCommerce Leading the Way?

According to data security industry publication CSO, physical retailers are struggling to keep up with online sellers when it comes to digital security. The reason for this may be found in the frequency of updates. eCommerce sites update their order and payment applications far more frequently than brick-and-mortar stores. Just as important is the fact that retail chains take far longer to respond to multi-store attacks, which makes them much juicier targets for attackers.

The biggest threat facing eCommerce sites seems to be DDoS attacks that are launched through media consumers who are unknowing and unwilling participants in the attack. The most powerful tool that the industry seems to have at its disposal is mutually beneficial data sharing that informs every business in a pact about the nature and type of attack suffered by any one member of the group. The good news is that for all the increasing attacks facing eCommerce sites, the industry's situation is much brighter than that of their cousins in physical retail.

About the Author

Nick Rojas is a business consultant and writer who lives in Los Angeles. He has consulted small and medium-sized enterprises for over twenty years. He has contributed articles to Visual.ly, Entrepreneur, and TechCrunch. You can follow him on Twitter @NickARojas, or you can reach him at NickAndrewRojas@gmail.com.

DEFENSIVE CYBERSPACE
Operations & Intelligence

THE ANNUAL INSS-CSFI CYBER CONFERENCE APRIL 27–28, 2015

APRIL 27, 2015
8AM-5PM

Ronald Reagan Building and International Trade Center
1300 Pennsylvania Avenue, NW
Washington, DC 20004

APRIL 28, 2015
9AM-5PM

Solution Panel, Workshops & Exhibition
The George Washington University
City View Room
1957 E Street, NW | 7th Floor
Washington, DC 20052

Speakers will include top-level U.S., Israeli, and international technology experts and government officials leading the next wave of cyber intelligence and defense innovation.

THE CONFERENCE WILL COVER THE FOLLOWING TOPICS:

- Cybercrime and cyber terrorism
- Cyber defense law and policy
- Cyber intelligence
- Cyber operations
- National policy and strategy
- New defense technologies
- TOR – the Black Net Challenge

For more information, please visit: **www.DCOI.org.il**

To register, please visit: **cps.gwu.edu/DCOI_2015**

INSS
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
Cyber Security Program

THE CYBER SECURITY FORUM INITIATIVE

THE GEORGE WASHINGTON UNIVERSITY

CPS_1415_139

Why Cybersecurity is for CFOs too

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

In the past, business leaders often looked at cybersecurity as something the tech guys were supposed handle. After all, it's only the health of the IT infrastructure that's at stake in the event of a cyberattack, right? Not anymore.

Today, things have changed dramatically. Senior executives at enterprises in all verticals know that a breach isn't just a tech issue.

Losing company or customer data today could lead to major financial and reputational damage due to legal penalties and loss of public trust.

That makes cybersecurity a business-wide challenge, not just an IT one.

CFOs should have something to say about cybersecurity

It sounds odd to say that the head of finance should be part of the security team, but according to an op-ed by Steve Durbin, managing director at the Information Security Forum, in CFO, that's exactly where he or she belongs.

Durbin argued that the theft of a company's financial data - for which a CFO is directly responsible - can be absolutely devastating.

Insider threats that lead to the loss of funds or banking information are always a possibility and will have a direct impact on the business.

These, and others, are the kind of threats that the CFO should be aware of and help mitigate. The CFO must understand what information is within the network, how it's secured and how hackers could possibly gain access.

This cyber defense plan is a big part of what CFOs today will be required to disclose to the board in regard to the business's digital assets.

CFOs are taking up the charge

Fortunately, many CFOs already know that cybersecurity is of the utmost importance.

A Deloitte study from the third quarter of 2014 found that 74 percent of the 103 CFOs surveyed said cybersecurity is a top priority.

Specifically, they believed that protecting the network was critical for preventing their businesses' intellectual property, data and facilities from being compromised.

Cybersecurity is part and parcel of the senior executive's job today, and these executives can't just opt out of using the digital tools that underpin their entire operations.

As the consequences of a cyberattack have a ripple effect far beyond the IT room, it will be imperative for upper management to make cybersecurity a focus.

CFOs can help make the case for advanced cybersecurity tools that protect sensitive financial data from within the network, thereby defending it against both insider threats and rogue outsiders.

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 issue of cyber tracking in a modern consumer's society

Milica Djekic

It appears that an information is getting so vitally important for a life and business of the modern humans, so the places where people exchange their information are getting significant as well. As the most common way of the modern exchange of information, we would mention e-mail accounts.

They are so practical for an everyday's use and also very convenient for the different sorts of cyber devices. The main issue here would be that those accounts can be tracked or accessed in an unauthorized manner, so they could potentially be seen as a spot suitable for an information leakage.

In this article, we intend to talk about the challenges of cyber tracking as well as provide some practical advices how to protect a valuable information and cyber asset as same glance.

How a cyber tracking is possible

As it is known, many publically available as well as commercial e-services offer an opportunity to check someone's e-mail correspondence, once you obtained such login details. In fact, with someone's login information in your hands, you can access that person's e-mail account as well.

There are so many possible scenarios how those sorts of access could be misused for, say, a business espionage, cybercrime or even terrorism. Someone's login details are very confidential information and once they are in service of malicious actors, they can be used for obtaining a confirmed information on someone's personal or business activities as well as another habits.

It's not hard to imagine which sort of advantage on the market your competitors could take, once they get familiar with your business e-mail correspondence. Also, it's getting clear how risky is the situation when some criminal or terrorist groups are getting familiar with someone's activities through a cyber tracking of his e-mail account.

Finally, many confidential information get exchanged through e-mail correspondence and that communication asset appears as so suitable for hackers and the other cyber criminals to break into it and take advantage to such a content. So, a cyber tracking of your e-mail assets appears as a real nightmare, does not it?

In addition, what is also important to understand is that a tracking of someone's e-mail account is possible as well if some sort of the professional security e-mail checking tool is applied. This sort of software does not require an user to be familiar with someone's login details, but rather to know such a person's e-mail address.

You would realize how this can be risky if we deal with an open-society countries such as the western ones where many expert's, government's or business e-mail addresses got available publically through the web.

There are still many parts of the world that got untrusted and which could misuse those professional security applications, so it is strongly advised that a distribution of such tools should be better controlled.

Luckily, there are still some good ways to protect your e-mail asset and we would talk about them through this article.

The ways to protect your e-mail account

There are still many good ways to assure your e-mail asset. As we said before through our articles, there are two basic sorts of e-mail accounts: (1) cloud-based e-mail clients and (2) computer-based e-mail clients.

The both types of those e-clients got a quite good protection systems which are currently available on the market. For an average user and some regular business applications, they are quite reliable, but they still cannot guarantee an absolute security.

For instance, if we deal with a web-based e-client such as the Gmail, we can notice that we could access our protected e-mail account from many trusted machines as well as disable an option of the e-checking from a remote service, but what we need to login to such an account is a verification code which can be received on our cell phone.

You would agree that this method is still quite good for an everyday peaceful use, but in case of cyber wars when your opponents are trying so aggressively to obtain your confidential information, it's not that suitable.

Say, those bad guys got your cell phone number and they also have a software for a SMS tracking as well as your e-mail account login details; it's getting clear that they could easily try to login to your e-asset, send a request for your verification code and obtain it without any difficulties simply tracking your text messages.

Indeed, those folks could be located so easily and you would, nodoubtly, get an information on that login attempt and your web-based service would resolve such a concern for you.

But the headache is those bad guys would already make a breach and potentially change something within your cyber asset.

A modern security solution - safe and convenient at once

As it is known, nowadays we deal with so emerging age and many modern developed societies are the consumer's ones. The majority of people in such a world simply got that habit to have a convenience in their everyday's lives.

It's not that strange if we have in mind that today's developed countries are very technology dependent. The ultimate goal for current technological solutions is to be reliable and convenient as same glance.

A reliability means that an engineering product would be capable to obtain its defined performances under a very wide spectrum of circumstances and a convenience offers that a consumer would get pleased using such a solution.

It seems we could invoke the similar approach to security making its solutions safe and convenient at once. That would be a quite good way to follow modern trends in today's technologically developed human's environment, would not that?

So, maybe we could call that new age in a security a "tech-like security".

A tech-like security – is that the next phase in a security?

In our belief, this could be a great opportunity to try to discuss and define what this new term could cover. We could call it a tech-like security or a techful security, it's up to you! But, it's still a good idea to put an eye on it.

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.

Don't Let Human Nature Undermine Security: Brute-Force and Exploit Attacks

Imagine you are standing within the walls of a long hallway lined with closed doors on either side. One of those doors hides a valuable artifact, and you are presented with a keychain that holds several keys.

This scenario is an analogy for what happens in an information security event known as a **brute-force attack**. The attacker knows there is an important piece of information (the valuable artifact) hidden on a web server somewhere (the room). The attacker also has an exhaustive list of predefined passwords (the keychain) that they will try to use to gain access to the web server. The general idea in a brute-force attack is to attempt every password until the attacker gains unauthorized access to the server.

Now imagine all the doors have metal locks. Instead of trying every key in every door, you could just start checking if the locks are rusty or damaged, and try to force the doors open in order to get access. This is how an **exploit** or **vulnerability attack works**, by taking advantage of some flaw in the system to obtain unauthorized access.

In an exploit attack, you are relying on the weaknesses of the system itself (the rusty or damaged locks) to gain illicit entry. In this scenario, you have to hope that there is a flaw in the security plan to get in; an overlooked piece of infrastructure with a vulnerability, or perhaps a zero-day flaw threat like the Heartbleed or Shellshock bugs. But in the case of brute-force attacks the landscape is different. Here, the exploited vulnerability is a human one: the tendency to choose weak passwords.

Brute-force attacks are time and resource-consuming compared with an exploit attack. Depending on the system, the attacker will require anything from a couple of computers to a botnet of hundreds of zombie machines just to get started. Additionally, the attacker will need to plan how to hijack the system carefully, because there are extra security controls that emit warnings whenever there are continuous failed login attempts over a specific period of time. However, if a hacker doesn't have access to a zero-day vulnerability, a more complex brute-force attack will have to do, even if it has less chance of being successful.

The Door is Ajar: How an Attack Begins

In order to determine the method of attack, hackers assess the potential value of attacking a particular system based on elements like unpatched software, vulnerable operating systems and available remote access protocols.

There are several readily available tools hackers use to gain knowledge about a system. Through them, the hacker can learn about the operating system and version being used, the current set of open ports, the status of the firewall and other details that helps them discover accessible hosts on a network.

For example, the famous ***nmap*** tool lets you—among other things—scan the reserved TCP ports of the target system:

```
Not shown: 984 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   open   http       Apache httpd 2.2.15 ((Ubuntu))
|_html-title: HTML Title
110/tcp  closed pop3
113/tcp  closed auth
443/tcp  open   https
993/tcp  closed imaps
995/tcp  closed pop3s
5432/tcp closed postgresql
8080/tcp closed http-proxy
8083/tcp closed unknown
8086/tcp closed unknown
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
```

Once the attacker knows the particular vulnerabilities of a system, they can decide whether a vulnerability exploit or a brute-force attack would be more successful. If the system doesn't have any clearly apparent vulnerabilities, the latter attack becomes the more feasible option.

The cybercriminal will then start searching for an access point, which is normally a protocol used for remote control such as SSH (on UNIX systems) and RDP (on systems running Windows).

This is where the human element is so crucial in doing its part to prevent an attack. In many breach cases we have seen, system administrators didn't realize that remote protocols were active on their systems that enabled unauthorized access.

Easily guessable passwords like “admin12345”, “posadmin” and “qwerty”, are also used far too often, and make an attacker’s job a lot easier. For example, in a Linux server machine you can find the names used in failed SSH login attempts by running this command:

- grep input_userauth_request /var/log/auth.log

input_userauth_request: invalid user admin [preauth]
input_userauth_request: invalid user blank [preauth]
input_userauth_request: invalid user guest [preauth]
input_userauth_request: invalid user iclock [preauth]
input_userauth_request: invalid user ftpuser [preauth]
input_userauth_request: invalid user support [preauth]
input_userauth_request: invalid user operator [preauth]
input_userauth_request: invalid user ubnt [preauth]
input_userauth_request: invalid user default [preauth]

Additionally, you can get information on connections not related to login attempts, such as port scanning:

- grep "identification string" /var/log/auth.log

Did not receive identification string from IP1
Did not receive identification string from IP2
Did not receive identification string from IP3
Did not receive identification string from IP4

There are a handful of tools available designed to leverage log entries to deny access by dynamically changing firewall rules based on suspicious activity. A good example is *Fail2ban* (a Unix-based tool), which checks for practically any service that writes information about failed login attempts to a log file.

Bolting the Doors to Prevent Brute-Force Attacks

Over the years, a fairly common technique called ***Port Knocking*** has been implemented to protect against brute force attacks by disabling port scanning in the server machine. Port Knocking consists of closing all the ports of the server using firewall configurations while opening some ports based on a specific series of connections attempts (“knocks”) sent by the user—think of it as opening the door only after the third knock.

There had been some discussions in the industry about whether or not this technique falls into the category of “security through obscurity”. Despite the different opinions on this, the reality is that Port Knocking is another authentication mechanism with some important drawbacks:

- Single password authentication mechanism: all the users will be using the same password to open the ports and even though passwords can be changed, there is no easy way for the users to do so.

- Not ideal for protocols with high traffic.
- It can be target of replay-attacks: if someone can spy your connections, the “knocks” sequence can be easily deduced and used against the system.
- Some Port Knocking implementations used in production environments are open-source: the “knocks” sequence can be inferred by reverse-engineer the algorithm used by those implementations.
- Often when implementing a Port Knocking technique, there is a unique element monitoring the ports opening/closing operation, making it a single point of failure that may block the access to the server in case of failure.

Single Packet Authorization is a variation of Port Knocking that solves some of the challenges mentioned above, and it consists on reducing the number of sequence attempts to only one, using a single encrypted packet to authenticate the user that wants to open a specific port.

Whether Port Knocking or Single Packer Authorization or other techniques are deployed, some security implementations rely completely on Port Knocking to avoid brute-force or any other forms of attacks.

You Are Only Human, But the Devil’s in the Details

If the password for remote access is weak, it is much more likely to get hijacked even when a system is highly armored with restrictive policies. In addition to forcing the use of stronger passwords and two-factor authentication, systems administrators should ensure they are always running the latest version of any given software to minimize the vulnerabilities and maintain strong policies about software updates, including ongoing investigations about flaws in the software they are currently using.

Here are some good sources to check on software vulnerabilities at several exploit databases: https://cve.mitre.org/, http://www.kb.cert.org/vuls/ or http://www.cvedetails.com/.

Furthermore, be mindful of **Pivoting**, a technique used when hackers try to access different devises in an attempt to reach the most critical computer in the network.

The idea behind Pivoting is simple: why would you attack a highly restrictive server directly if you are able to break into the most vulnerable computer in the network and reach the highly restrictive server within the organization by *pivoting* from computer to computer? This is living proof that a security system is only as strong as its weakest link.

Of course, there are other types of attacks that exploit the human capacity to deliver privileged information to unauthorized parties, like social engineering and phishing attacks. Even though those attacks seem to be related to elements outside the direct configuration of your security perimeter, they can affect it right away depending on the information they allow to be collected.

We are only human, and as such, our security strategies can be undermined by the human capacity to make mistakes. Either way, there are methods to minimize the possibility that the human element enables exploit and brute-force attacks:

- Keeping your software up-to-date.
- Improving your remote access security using elements like two factor authentication for RDP sessions.
- Requiring the use of strong passwords or password managers.
- Limiting the number of failed login attempts to your systems.
- Restricting the number of users and workstations who can have access to remote sessions.
- Other best practices regarding reinforcing remote access control, can be found here: https://www.us-cert.gov/ncas/alerts/TA14-212A.

To err is human, and there is no way to completely eliminate the possibility of an attack. But reinforcing security policies, especially those involving human interaction, and having a plan B ready to go when mistakes happen is a divine best security practice.

About the Author

Luis Betancourt, Technical Product Manager, Easy Solutions

As Technical Product Manager for Easy Solutions' safe browsing products, Detect Safe Browsing, Luis and his team focus on the research and development of innovative anti-fraud technologies. He graduated with a Cum Laude in Mechatronic Engineer from the Military University New Granada. He currently lives in Bogota, Colombia

20 Ways to Keep Your Business Info Safe

Change Default Passwords

Update All Software Frequently

Install Anti-Virus Software

Keep Sensitive info away from employees

Make Password changes Mandatory

Keep Your Network Secure

Limit Employee Access to your Network

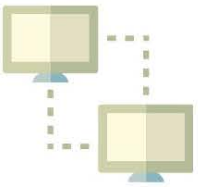
Keep office key holders to a minimum

Brief All Employees on Data Protection

Install CCTV on your Premises

Lock Away Sensitive Data

Shred All Confidential Waste



Ensure Firewalls are Secure

Outsource Your Security

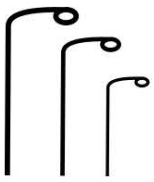
Carry Out Background Checks on Staff

Ensure Windows are Locked

Change Passwords etc when Employees Leave

Promote Security in the Workplace

Be Careful when Opening Zip Files



Have adequate Outdoor Lighting

HOMESHREDUK
the home of shredding

Sources:
http://www.smallbusinesscomputing.com/webmaster/article.php/3908811/15-Data-Security-Tips-to-Protect-Your-Small-Business.htm
http://www.markeluk.com/useful-information/8-tips-to-keep-your-office-secure.aspx

If a college student can do it…

Imagine this. A local student is getting ready for a presentation about recycling in your office. Within 15 minutes he has already found a backdoor to your computer, your username and password and has already walked out the front door. You don't know his name, where he comes from or where he's going. All you can really say is that he seemed so nice, and just needed time to prepare his presentation. Who you thought was a college student, really turned out to be a hacker and he's just walked away with more than your username and password. He's just walked away with your life.

On April 2015 I was approached by the owner of a local company in my city. He knew that I was a student at Dixie State University, and that I wanted to explore the aspects of becoming a penetration tester (this is known as a security tester through ethical hacking). He wanted me to check how secure his system was, through accessibility and vulnerability as well social engineering (talking to people seeing what information they will give me). We wrote up a contract with his personal contact information as well conversed with his head IT administrator in the case I got caught, I would have something to show that I was not a real hacker. I laid out the following goals in my assignment 1. Get direct access to their switch/router, 2. Find vulnerabilities, 3. Verify the ability to open back doors for secure access and 4. Leave without a trace.

In preparation of my tasks, I made a list of tools that I would need to aid me the hack. It is important to note that these tools can be easily acquired and without the right protection, can wreck havoc on not only your office but your home as well.

The first tool I grabbed purchased was the Pineapple router. The pineapple router is one of the best tools for an evil twin and a man-in–the-middle attack. What set's the pineapple apart from normal routers are the infusions that come preinstalled on it. The three tools I used from the router were SSL (secure sockets layer) strip, Karma and Beacon response. The best way to explain what an evil twin is to understand how a normal wireless device connects to a network. When you first connect to a network it stores in its settings the network name and authentication, and is saved as a trusted network.

Then when you walk into your home your router sends out a beacon to the devices in the home asking them if they want to connect, your devices then see that your network; has been used before, is trusted, and sends a response back saying "Yes I would like to connect online", and automatically connects to that network.

Beacon Response and Karma send out a beacon to all wireless devices no matter what your network name is and say "Hey I am your trusted network, you should talk to me first" your device then says "are you a trusted a network?" finally the beacon response replies back "I have the same network name for the network you usually connect to and you don't even have to tell me your password" and thus ensnares the victim.

The man-in-the-middle attack is used when combined with the SSL strip infusion on basic HTTPS (Hypertext Transfer Protocol Secure) websites. HTTPS is a internet protocol we use when logging on to a secure website. Whenever you see a lock in your website URL or that the URL starts with “https:” you can be assured that your information that you send to your bank, Facebook page, or any other secure website is encrypted. However, what the SSL strip does is it turns a secure website HTTPS to an HTTP thus sending your information in clear text. There are exceptions for this when the SSL is built into the code of a website, however for this company attack I was not too worried about that. The pineapple router could also let me poison websites that they frequently visited. How it poisons is it sets up a page to look exactly what you are looking for but it sends the credentials back to me, rather than the real page.

The next thing I grabbed was the operating system Kali linux. Kali linux is an operating system most penetration testers use as it’s highly versatile with many of a penetration attacker’s tools, as well has preinstalled packages to attack any system. The two tools I will be talking about, installed on the Kali Linux operating system, are Armitage and the social engineering toolkit. Armitage is a tool developed by Raphael Mudge, to help penetration testers do scans and get exploit recommendations.

The social engineering toolkit is toolkit that sets up attacks for you through an easy user-friendly interface. Although there are many uses for the social engineering toolkit, such as poisoning a USB to install malicious code on your computer, I used its ability to make a phishing email that would capture the credentials of a user.

Next was the USB rubber ducky. This is a programmable usb that when plugged into a computer, it auto runs its program to harvest credentials of clients and emails them back to the attacker. The program I was going to use was called WebBrowserPassView. This is a program made by Nirosoft to grab all the websites you have visited with cookies. Which means, it captures your username and passwords if you’ve ever told a website to remember your credentials.

The last thing I needed was a new identity and a five dollar smile. The problem with my pineapple router, (although I can log into it remotely), was it had to be in the vicinity of the companies wifi. So I came up with an idea on how to sneak it in. I would say that I was a representative from the recycling group at the local college. I figured I could drop bins off with the router on the bottom of the bin with an external battery, that way when or if I ever made a change on the bins I could easily retrieve it. Oh who doesn’t trust a nice smile?

I went to one of the owners offices and told them and that I was from the local college and for our recycling club we were going to different local business and were placing recycling bins to help the environment as a service project. I told them that I had spoken with the owner of the company who said it was ok and that I had a short presentation that would be followed with some pizza.

They seemed reluctant about the presentation, but after telling them I had spoken with the owner and he okay’d it, they accepted. I showed up the next day, a half hour earlier, then

expected, and asked if I could have some time setting up. They told me it would be fine to which they offered me a personal office as well as a drink and that's when I went to work.

Plugging into their network, I was able to run Armitage and started a scan. While that was running, I booted up my router, and added an antenna to give the router a chance to talk to wireless devices outside of the network before they connected to the real network. I connected to their wifi, there was no password for their wifi, as only their clients are the ones that connect wirelessly (and a few employees breaking the rules). I was able to set up my router and start catching information because there was no protection. It was a slow day so there was not much to catch. I figured I could just drop my car off into the parking with my router for a week and let it capture all traffic coming in, but after meeting the criteria I stopped.

Due to the nature of the contract made, I was not able to record what private information I gathered, as I'm a college student who didn't need the bank account information of their cliental. I was there to plug in the holes of the dam, not see what made them. I tested their website using their email address (as a username, I didn't know what else to do but knew emails are common usernames to logon pages.) and a made up password to see if it was vulnerable to the SSL strip, which it was but more important, they didn't have SSL security for their logon page.

Because of this SSL strip was unnecessary and I was able to catch the password and user name in clear text anyways. My scan using Armitage showed me several programs not updated, and gave me a list of exploits I could use at the click of the button; however I just had Armitage run me a vulnerability report instead. After making the report, I thanked them for the water and left. Without my real contact information, and having walked there, there was not a way they could trace back to me. I had fulfilled my mission, 1. Get direct access to their switch, 2. Find vulnerabilities, 3. Verify the ability to open back doors for secure access and 4. Leave without a trace.

About a half an hour later I explained to the owner what I had done, and suggestions on how he and his employees could guard themselves better in the future. "They were just being nice" he told me, I responded back "They were being too nice" they 1. Trusted someone that they didn't know, 2. Gave that untrusted person an office to work in, and 3. Left me unattended. The owner said that they thought it was suspicious I was plugging into the wall with my Ethernet cable, to which I responded "That is very suspicious, I'm very glad they didn't stop me."

However, I wasn't done. I then crafted the following email to all the employees:

There has been an update to the policy on Holiday pay. Sorry for the inconvenience but lot's of people have been abusing it lately. --- Owner of Company

Phone number to local pizza place

Please login here to review the policy.

www.thecompaniesnamecom/login.php

This was an email that took them to an identical fake login page that would pass me the credentials. Although it was functional I showed the owner of the company asked me not to do it. As he's the client I did not. I did however send it to him and it was marked as a phishing email so they were able to verify the integrity of their email system.

Next I knew that they at the main office they used TeamViewer to see what their employees were doing on their computers. I decided to make a few phone calls to their receptionists. I told them that they were in trouble as the main office got DMCA notices saying that someone in their office was illegally downloading movies, and so we needed to log into their computer to see if it was them or not. With a few phone calls I was able to get a 2 out of 5 of the TeamViewer numbers I needed to log remotely into their computers.

Lastly I never got an email back from my ducky. Which could mean one of three things. 1. It failed, however I tested it several times and received results back. So the next two options were 2. They never plugged it into their computer to find out who it belonged to and which I had hoped would happen. Or 3.

Their computer wasn't running in administrator mode. This is good for two reasons. One of the main reasons why computers get viruses is because when you are the administrator of your computer, programs automatically install themselves without a prompt. That's why some times you see programs on your computer that you never installed. However when you are just a normal client, your computer alerts you that a program is trying to install on your computer. In fact Microsoft has said that 90 percent of viruses can be avoided on their computers when it is run without administrative access. Either way my ducky failed.

After my experience my recommendations to protect your own company as well as your home are as follows.

Place a password on the guest account wifi. Although the employee's computers are hard lined into a switch, the customer's information is as vitally important. I was able to set up a rouge access point within moments. Another good practice is to have a Rouge Access Point Detector. Make sure in your network security settings, you have a Rouge Policy set up with a timeout. Let's be honest, it's a little unrealistic have someone monitoring this, but its convenience vs. security.

Block Ethernet ports. Ethernet ports in a crowded lounge provide the attacker a chance to plug into your LAN (local area network) directly and run scans. In the case of Armitage, I was able to see what computers were assigned what IP address's and by running a scan of ports and services, see the vulnerabilities, and had the ability to run the custom attack against that machine.

Use MAC address filtering on a switch/router. Every device has a serial number built into known as a MAC address. With MAC address filtering you are able to prevent unwanted "guests" from tapping directly into your network, kind of like how you block phone numbers.

User education. Very rarely does the prince of Nigeria get dethroned (though it seems like it's happening more and more often to him, poor guy) and then contacts you with a way to get him home. Although we are slowly adapting to such an attack, it would be wise to login into your login page directly, or hover above the link and see if it takes you to an IP address's rather than a known domain name. In my email I changed the link to look the same as the login page to trick customers, but could have been foiled had they looked at where the url would have taken them. Also, don't stick any foreign thumb-drives in the computer and execute them. I do not want to sound paranoid and say every lost thumb-drive is a hacker attempting to get in, but if you have things to protect than you should act like every lost thumb-drive is an attacker to get in.

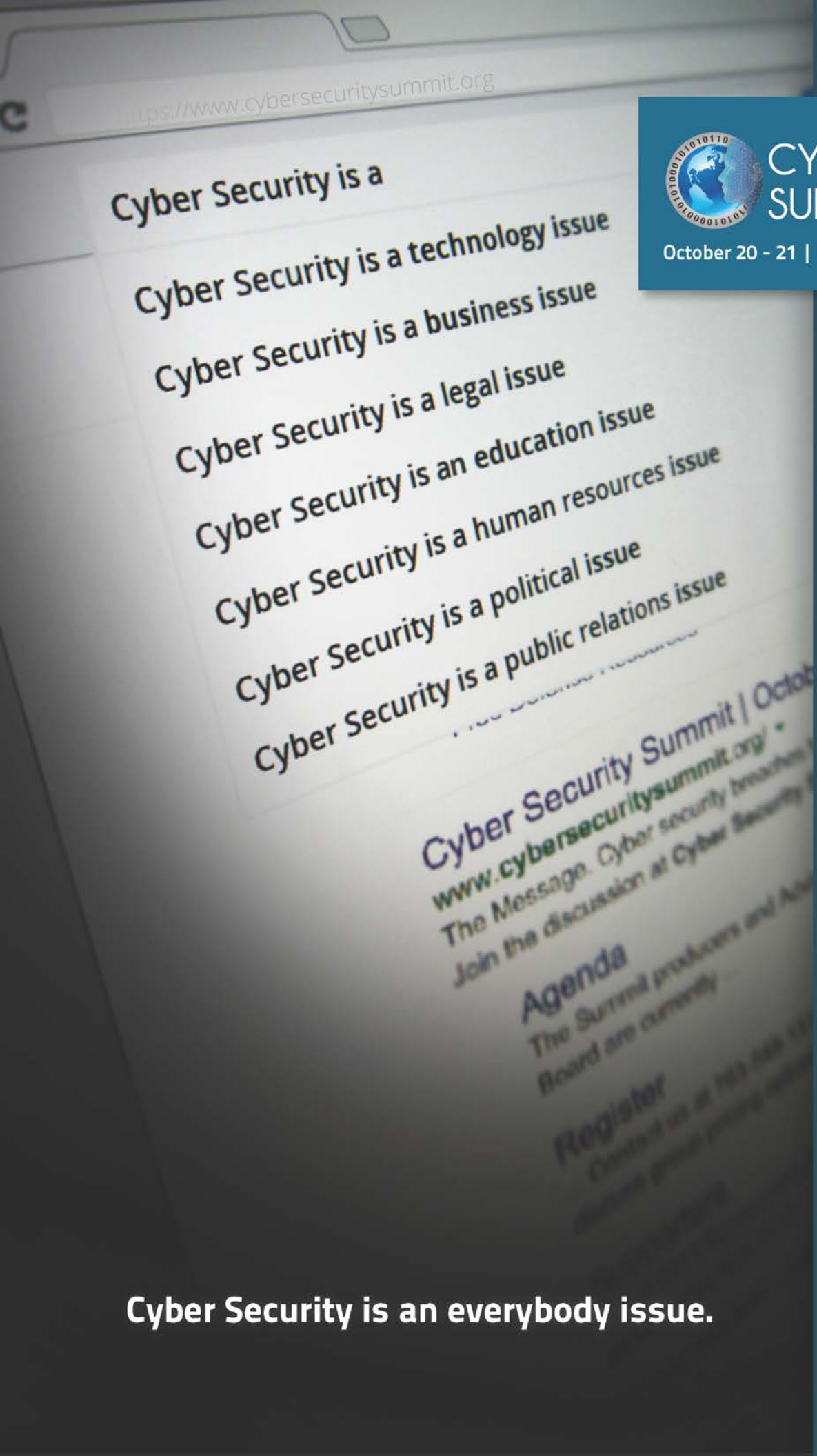
Run computer without administrative access. As stated before this is a very efficient way to avoid malware being installed on your computer.

Have a keyword. It's easy to call anyone and tell them their job is at risk. It's the fear that get's people to show that they are innocent and therefore they are willing to do whatever it takes to save their job as quickly as possible. However, it's important to verify who is on the other line of that call.

Remember, there will always be some risk and vulnerability to get into your system. If you have the best security system in the world, odds are you won't be able to get any work done. It all comes down to productivity/connivance vs security, the best way to protect your self are, protecting your location, through blocked ports, MAC address filter, verifying identities, and user awareness.

About the Author

I am a Saint George resident currently attending Dixie State University, in Utah, with the expectation of graduating in the fall semester with my major in Informational Technology and Minor in Digital Forensics. I will be applying for graduate school this upcoming year to earn my master's degree in Advanced Security and Digital Forensics.



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

"Man Over Machine"

Brian Beyer, co-founder and CEO, Red Canary

When faced with an emerging threat or visibility gap, we in the security industry have a tendency to look first to hardware and software for a solution. Humans at this point seem to be an afterthought in the data security wars.

This machine-first trend is clearly visible in the marketing material for many new and well-established products and services that promise full solutions in a box, even in the fact of very dynamic and varied environments.

Often, these providers attempt to be everything to everyone, with a veiled implication of the proverbial "silver bullet" to anyone's security problems.

It's true that researchers are making impressive advancements in machine learning, artificial intelligence, and similar technologies from the science fiction of recent past.

But this approach also introduced the disturbing practice of over-alerting from many security vendors. They often err on the side of caution, which minimizes the chances of an actual malicious event going un-alerted.

The market trend toward these ends is visible today. However, it is a deeply flawed one because such solutions ignore the simple reality that our attackers are humans - and 200,000 years of human history has shown us that we're pretty good at adapting to survive impediments in our path.

Consider that the commercialization of any technology-based solution takes a lot of time - a period during which the attackers are advancing as well.

As we've seen with the rise and fall of Antivirus, signature-based intrusion detection, and other protective solutions, even a low-grade attacker can easily thwart such solutions soon after deployment.

Another way to look at this comes not from the information security sphere, but the world of competitive chess. After the famous "man vs. machine" matches came the concept of "Advanced Chess," which demonstrates that even a moderately-skilled human paired with a computer gains a tremendous strategic and tactical advantage over a supercomputer alone.

There is some integral notion of human intuition that cannot be modeled. Of Advanced Chess, Indian grandmaster Viswanathan Anand said:

"I think in general people tend to overestimate the importance of the computer in the competitions. You can do a lot of things with the computer but you still have to play good chess."

In a classic example of this concept, Google created a 16,000-processor neural network that correctly identified cats in YouTube videos 75% of the time. This is not poor performance, but consider that a two-year old human can perform the same task with near-100% accuracy.

So while machines will continue to improve, there is a vast collection of tasks for which humans will be far more efficient. A combination of solid technology, paired with a highly-optimized workflow for human vetting provides the best possible chances for success against dynamic and dedicated attackers.

Humans are far better at determining if a series of observed events in a potential victim's environment are truly malicious, or simply a coincident series of benign activities.

This unified approach is far more effective than traditional attempts at silver-bullet solutions, as the human provides critical differentiation between "good" and "bad" observations.

The efficiency for such a unified solution skyrockets even further when the human portion of the process is enhanced by multiple machine-aided classifications such as behavioral observations, static and dynamic binary analysis, and cyber threat intelligence.

Thankfully, this trend toward leveraging human power with that of machines is gaining favor, from some of the largest companies like Dell SecureWorks to newer service providers like Hexis Cyber Solutions and Masergy already incorporating human analysts into their threat detection services.

Even Verizon and other large MSSPs have seen the light and are incorporating humans into their services.

This begs the question of how a security team or provider can fuse the technology and human components into a credible solution. First, they must evaluate multiple observation and collection platforms. These may span the space between endpoint, network, log aggregation, and other solutions.

With the collected data from the platform or platforms they select, the team then evaluates and selects one or more intelligence sources that can effectively enrich the collected data, directing a human's precious time and attention to legitimate or likely threats.

Human analysts need to be continuously trained on their portion of the workflow as well as the ever-evolving threat. This likely involves typical workforce training but also an awareness among peers to maintain currency.

That awareness must span the entirety of the information security threat space as well as industry-specific knowledge bases to be most effective and accurate. They require a streamlined workflow to ensure high efficiency, so the organization must invest into the research and development of the workflow itself and any supporting technologies.

As you can see, even the automated component of the machine-human hybrid approach is a massive undertaking. The human component makes this significantly more complex and expensive - but both are absolutely required to build a competent security solution.

While machine technology will improve in the future, so will our adversaries.

Humans will remain a critical component in this process. Their roles will change as better technology can assume portions of the process, but the day for a technology-only threat identification solution is still too far in the future to realistically predict.

Instead of seeking a technology-only solution, information security organizations must recognize that humans are a critical component in the overall threat detection process, and seek solutions that mesh the strengths of both technology and humans in a meaningful and cost-effective manner.

About the Author

BRIAN BEYER, CEO/CO-FOUNDER, RED CANARY

Brian leads Red Canary to deliver its mission of bringing world-class threat detection and response to every business. Prior to co-founding Red Canary, Brian incubated cybersecurity products at Kyrus, innovated big data processing solutions for the intelligence community at Northrop Grumman and started his career in cybersecurity at ManTech. He can be reached at brian@redcanary.co.

Social Engineering Tactics: Reporting from the Front Line of Breach Defense

By Michael Buratowski, Vice President of Cybersecurity Services, General Dynamics Fidelis Cybersecurity Solutions

Social engineering is all about presenting information that causes someone to take action. This may mean getting a victim to open an email attachment, click a link or even plug in a USB that appears to be misplaced. Unfortunately, some companies are making it even easier for social engineers to target their employees by having proprietary information, such as staff listings featuring personally identifiable information (PII), who employees report to, and job responsibilities, easily accessible online. This kind of personalized information is exactly what is needed to piece together a believable story that causes the victim to engage.

Social engineering tactics can take many different forms. Outlined below are some common scenarios that companies are running into and tips for preventing damage when encountering them.

Scenario: An attacker loads a PDF with malware that will deploy when opened. Through a spear phishing tactic, the attacker spoofs the sender's email address to look like a legitimate contracting firm and sends the email to a contact in business development. Because business development departments are used to seeing and opening documents like contracts and RFPs, the attachment gets opened and the malware is deployed.

When people consider phishing attacks, the "your friend is stuck abroad and in need of a wire transfer, please send banking information" types of emails may come to mind. However, today's attackers are smarter – they'll do a bit of research and figure out exactly who their target is, who would be most likely to send that target an email and exactly what to send them to get them to do what the attacker wants.

Lesson: Don't limit cybersecurity training to the IT team. Providing basic training to all employees is absolutely critical, as threat actors will often target non-IT employees, assuming they are the least experienced with recognizing these attacks.

Scenario: An attacker infiltrates a company using very advanced malware. While the company is in the process of shutting down their attack vectors, a non-IT employee receives a call from someone identifying themselves as working with CISO on a new project – the breach – and asks for the names of all the outside contractors working on the project.

Attackers don't always sit behind a curtain, sometimes they'll be forward in the steps they take to confirm whether their breach has been recognized and to determine the level of breach defense and remediation they are up against.

Lesson: Ensure all employees have a heightened sense of awareness and sensitivity to questionable requests like these and are prepared to deflect the situation by either directing requests to the IT department or even playing dumb. “I don’t know” can be an answer when talking to a social engineer.

Scenario: An attacker physically places a USB drive near the entrance of a company. An employee finds it upon arriving to work in the morning, and in order to identify who it should be returned to, plugs it into their laptop.

While good natured actions like trying to identify the owner of lost property is usually rewarded, in the case of protecting your company’s network, it can be the reason an attacker is able to infiltrate.

Lesson: Don’t connect your computer to any unknown USBs, external hard drives, etc. because it can be much more harmful than you think. Shamoon and Dark Seoul both started this way. Once the malware is introduced, it can propagate like mad.

No matter the social engineering tactic, attackers are persistent in how they research victims to ensure their story is believable. Companies should put all employees through rigorous security training and be mindful of what information is publicly available, since something as simple as a name next to a job description could be the bad guys’ ticket in.

About the Author

Mike Buratowski, Vice President of Cybersecurity Services, General Dynamics Fidelis Cybersecurity Solutions, manages the efforts of the General Dynamics Fidelis’ Network Defense and Forensic Services team – which has investigated more than 3,500 breaches – to help customers prevent, contain and remediate breaches, along with providing forensic evidence for the prosecution of cybercriminals. He has also served various operational roles within the Department of Defense’s Computer Forensics Laboratory, including examiner in the Major Crimes & Safety section. Additionally, he managed the US-CERT contract, where he led efforts in improving the nation’s cybersecurity posture and managed cyber risks facing the nation.

Preparing for Opportunistic and Targeted Attacks Requires Sound Leadership

By Mike Sconzo, Senior Threat Researcher, Bit9 + Carbon Black

A shift is occurring in information security. Security leaders are not only looking to increase their detection and response capabilities, they are also bringing in security professionals with unique talents who can hunt for new incidents and respond to them. Security is no longer simply about technology. Now, it's all about people and processes powering technology. The "people" element is, perhaps, most important.

The move toward active detection (hunting) and response is a necessary change throughout the industry brought on by the mindset shit of "I hope my organization won't be attacked" to "when and how frequently will it be attacked?" In preparing for the "when," all is not lost. By understanding how your organization falls into each target group, it is possible to defend, detect, and respond against the two types of attacks organizations normally see: opportunistic and targeted.

Opportunistic Attacks

There are various ways to become a victim of opportunity. At one end of the scale there are traditional commodity malware and exploit kits. These are distributed with very little regard for who or what gets targeted, and the attackers' goals often vary – perhaps the malware gathers credentials to banking or gaming sites, mines bitcoin, or various other purposes.

There are several popular exploit kits, and campaigns vary in type of malware distributed. According to Malwarebytes, about two thirds of new malware infections are delivered by exploit kits.

Taking this number and looking at the total number of malware events in the Verizon Data Breach Investigations Report (170 million), leads to at least 112 million malware infections this past year by exploit kits, like the angler exploit kit that was recently used in a hacktivism campaign to drive views to politically sensitive videos.

On the other end of the spectrum of opportunistic attacks are watering holes. The purpose of a watering hole is to compromise a site (the watering hole itself) in hopes that users of various other targets will visit it on their own.

Another example of an opportunistic attack, somewhere in the middle, would be scanning hosts on the Internet or using a search engine to find vulnerable software versions to exploit, like the notable cases of Heartbleed and Shellshock.

Since these types of attacks are based on availability and numbers, they occur quite frequently. In our honeypot network, we see over 100 thousand scan attempts in a 24-hour period. To assume that scanning and opportunistic exploitation of services doesn't happen would be naïve.

To thwart opportunistic attacks, defenders should make sure to “block and tackle” by keeping client and server software up to date, establishing good endpoint and network level visibility, and using mitigating controls (e.g., web proxies, firewalls). Adding hunting to discover incidents that may be missed by traditional technologies is also becoming increasingly important.

Targeted Attacks

When an organization is targeted for a specific reason (financial gain, intellectual property, etc.) it’s a mission, and therefore the level of attack sophistication can vary. The methods of the initial attack, and follow-on activity, can help understand the group (or groups) involved.

Since the initial foothold is generally not the source of information desired in the incident, attackers will move throughout the environment. During this movement user accounts will be compromised and privileges escalated, which is the lateral movement many organizations are concerned with.

After an initial attack is successful, it’s not uncommon for attackers to use various persistence methods in order to get back into the organization with the desired access to make future ingresses easier.

While attacks of opportunity generally have smaller reconnaissance to targeted attacks, both will pass through the various stages of the “Cyber Kill Chain.” This process is important in understanding where risk lies as well as the size of the attack surface.

While the same technologies can be used to cover both opportunistic and targeted attacks, the vast majority of technologies are weak in detecting targeted activity. Hunting and response play a much larger role in targeted attacks. Visibility is of the utmost importance.

Getting-high fidelity information from endpoints, network devices, and various server and application logs is crucial to minimizing the time to detection and response.

Breach Planning

Organizational maturity goes a long way in closing security gaps that may exist on an enterprise network. Examples of having a mature security organization include focused leadership, increased monitoring, targeted technology investments and effective policies and procedures.

Leadership should understand the various dynamics of the threat landscape to set direction and create policies and procedures to handle technology purchases and incident response

processes. Policies and procedures should guide technology purchases as well as enable effective response and feedback from an incident.

These aren't the kind of checkbox-style policies that various compliance frameworks require. Instead, focus on how to make best use of everybody's time and expertise. Not only should procedures be focused on breach prevention, they should also provide a roadmap for navigating issues that tend to crop up during breach response and remediation.

Another important element for strong leaders is the ability to build out a team capable of addressing the risk areas and performing advanced analysis. An advanced team needs good visibility to be effective. In order to get increased visibility, some technology is required. Being able to understand what's going on throughout every level of the enterprise, from endpoint to network, is important.

Technologies that promote visibility are crucial to risk mitigation and reaction during a breach. It's always important to learn from breaches. Teams should have a mechanism in place to gather feedback after an incident.

Learning what series of events led to the initial compromise is a critical part to the maturity process. In addition to understanding the cause, having insight into the organizational successes and failures will lead to more wins in the future.

For security leaders, it's important to understand what responses you want to issue internally and publicly. Just remember to remain level-headed and calm. While experiencing a data breach is never fun, it has become a part of doing business.

Don't rush into things, and keep a clear head when making decisions. By understanding the type of attacks, avenues for readiness and maintaining composure, you'll be best prepared to handle incidents of any type.

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**

Protecting Against New Security Weaknesses in Facebook

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

Much has been written about how the human element can be the weakest link in the security chain. Lack of awareness or a single lapse in judgement and the attacker is in. New Facebook vulnerabilities are just the latest example of how attackers are targeting employees to infiltrate corporate networks.

Security researchers at WebSegura found two different security issues in Facebook's API that could allow a hacker to plant malware on unsuspecting users' machines when they log into their Facebook account. For businesses with employees who check their profiles during the workday, this looks like yet another attack vector for hackers to exploit.

The two threats identified could have disastrous implications for businesses. One vulnerability allows hackers to plant malware on the user's machine by sending a link that appears to be from a trusted domain. In this case, the user receives an offer for a download that looks like it's from a trusted Facebook domain. If the user agrees to the download, a malicious user could gain control over the victim's computer and use it to launch attacks on the network. The second attack method targets Facebook users who haven't updated to the most recent version of Internet Explorer and exploits a vulnerability that allows them to download a link that contains a malicious file.

While these new weaknesses have only recently been discovered, the principles behind them are the same: Hackers are finding ways to breach a business's perimeter defenses undetected by exploiting credentialed users' lack of awareness or training. Whether it's a classic phishing email or malware sent through a hacked Facebook API, cybercriminals are becoming increasingly adept at breaking in without a trace.

Given Facebook's prominence for both sanctioned and unsanctioned use within a business network, this new attack vector is troubling. With insider access, hackers can install malware on a business's devices that could give them access to critical company, customer or employee data. The costs of these attacks can be sky high, due to complications such as legal repercussions and a damaged reputation.

Malware attacks through security loopholes are common, and organizations need to adapt accordingly. Here are just a few steps organizations can take to reduce risk:

1. Employee training is critical. Gartner finds that only one third of enterprises will spend resources on training which include social engineering and awareness. If employees are properly educated to spot potential attacks and social engineering techniques, they can become an organizations' first line of defense. Companies like PhishMe offer interesting solutions in this area.

2. Patching vulnerabilities and updating systems can go a long way to combat prevalent attacks. *The Cisco 2015 Annual Security Report* finds that attackers are targeting the most common vulnerabilities first and using them to penetrate corporate networks. Prioritizing and patching those top vulnerabilities quickly should be standard operating procedure for every IT Security department.

3. Blocking social media sites or prohibiting certain kinds of activities from the workplace, like posting, while not popular with employees is also an option.

4. Realistically, education, patching and blocking can't prevent every attack. It is also worth investing in security tools that enable continuous monitoring of endpoint and network activity and automated threat removal. These measures will make it possible to mitigate attacks that circumvent perimeter defenses and prevent major damage to the business.

Attackers continue to change their methods of attack. Security professionals need to be just as proactive, using a combination of tools and techniques to combat the latest round of threats swiftly and effectively.

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

Mobile Call Interception Threatens Law Enforcement

Despite the efforts of law enforcement and government agencies to conceal their use of IMSI catchers (also known as stingrays) this cat is long out of the bag and several miles down the road. However, what the somewhat outraged general public may not understand is that this mobile call interception technology has already evolved to the point where it is affordable to many people and organizations around the world, not just first-world government agencies. Mobile call interception devices can now be easily built and assembled by non-government personnel with decent technical know-how. It is frightening to think that criminal organizations now have many of the same surveillance capabilities as the authorities do. So, what does all this mean for law enforcement itself?

Criminal Enterprises & Mobile Surveillance

Criminal organizations have always gathered information on innocent people in order to extort them with kidnapping for ransom, blackmail, and other threats. Through mobile call interception, these criminals are even more empowered to gather valuable personal information such as the names and locations of family members and the daily activities of the target and those closest to him or her.

This is especially disconcerting for anyone working in law enforcement. Not only does mobile call interception place authorities in danger, but it puts their family members and friends in harm's way as well. With this surveillance technology, criminals can easily discover who's working undercover and who they need to extort to get what they want.

Also, major terrorist organizations like ISIS and Al Qaeda that have deep pockets are more than capable of using the same mobile surveillance equipment against the authorities that are trying to stop them.

The Common Use of Stingrays

The existence of unidentified rogue cell phone towers around the U.S. **was reported** last August. These rogue towers, also known as IMSI catchers, not only capture International Mobile Subscriber Identities (IMSIs), but they are also capable of call surveillance and SMS interception.

These rogue cell phone towers are just the tip of the iceberg. There are surely many more out there, and these fake mobile towers definitely aren't only in the U.S.

Mobile call interceptors are manufactured and sold abroad, and in most places, common criminals are making significant use of them. For instance, over 1,500 people were arrested in China last year for using IMSI catchers to spam people via SMS.

Criminals attempted to extort citizens with messages that appeared to come from banks, government agencies, and customer service departments in order to obtain valuable personal information. In addition to the arrests, Chinese authorities seized equipment from 2,600 fake base stations, according to the English Chinese news agency ECNS. If common criminals can extort the public with mobile interception in China, it is certain that this same equipment is being used by Chinese spies, spies from other countries, and countless others committing corporate espionage right here in your back yard.

Although long overdue, the FCC is finally beginning to **investigate the use of IMSI catchers** by criminal organizations. Luckily they will also investigate weaknesses in our mobile networks and try to remedy the problem from a network perspective.

Your Protection from Criminal Surveillance

The bottom line: law enforcement needs to ramp up their mobile counter surveillance and be able to protect themselves and their loved ones by detecting mobile call interception. Luckily, there are new products out there that meet this critical need for protection against criminal surveillance.

The **Network Guard** product line by Charon Technologies consists of some of the most innovative and comprehensive counter-surveillance products on the market. The Network Guard system is capable of detecting all types of network interception, from basic IMSI grabbers to advanced technologies that only governments possess. It also monitors all types of networks from 2G to 4G, LTE and CDMA.

Charon also provides another counter surveillance solution to law enforcement and mobile network operators with **Cell Seeker Pro**. Cell Seeker Pro can survey and map out entire mobile networks.

These mapped out networks can then be compared to maps of legitimate networks to determine the existence and location of poor reception areas, rogue base stations or IMSI catchers, and compare against suspected nefarious activity for mobile forensic purposes. Charon's mobile security products are an excellent solution to mobile call interception that can protect government and law enforcement agencies, and ultimately, the public itself.

About the Author

Scott Aken, Senior Director of Strategic Programs, Charon Technologies

Scott is a former FBI special agent in cyber counterintelligence. He has over 15 years of experience in IT, security and business strategy. As a recognized thought leader in cyber operations, his expertise is sought at government and commercial conferences as well as from notable security and technology publications.

Risky Business: Phishing and Smishing

By Joe Ferrara, President and CEO of Wombat.

Phishing and smishing (text message phishing) attacks are pummeling email accounts worldwide, and it's foolish to believe that all are as transparent as the Nigerian prince scam (which continues to bear fruit, by the way, in old and new forms). A good many of these messages are extremely sophisticated and difficult to spot — and they're winning at a high-stakes game. A recent Kaspersky Lab study, *Financial Cyberthreats in 2014*, revealed that just under 30% of the phishing attacks the company identified in 2014 were designed to steal users' financial data. An even greater threat to organizations are the fraudsters who want to gain access in order to steal intellectual property (IP), amass customer data, acquire insider knowledge, or wreak havoc on networks and systems. Case in point is the recent attack on the White House, in which Russian hackers allegedly gained access to the unclassified (but still highly sensitive) "Executive Office of the President" network by way of a compromised State Department email account.

How to fight these pervasive threats? As Andrew Walls, a vice president at Gartner, Inc., told TechTarget, "Employees can play a major role in detecting and responding effectively to social engineering threats, but the most effective approach is to combine employee-based risk management with automated, infrastructure-based risk management."

We agree; but as we've noted before, not all security awareness and training programs deliver the same level of risk reduction. The White House compromise is an excellent case in point; as Nextgov reported, a phishing email workshop had been offered to personnel in March as part of a yearly training series, *Cybersecurity Online Learning*. According to the Nextgov article, "All federal security employees were invited to participate in the 90-minute online training session. But no one from the White House watched."

Clearly, providing training that end users don't see is akin to providing no training at all. But we can't say we're surprised to know that people who were given the option of attending a 90-minute session chose to decline the invitation.

Three Tips for Reducing Risk

Phishing and smishing threats are likely to persist for years — if not decades — to come. But the risk you face from these threats depends on your infrastructure and your employees. Our Continuous Training Methodology takes a unique, 360-degree view cyber security education. One-and-done methods and once-a-year mammoth videos and presentations aren't as effective as our interactive approach, which delivers "bite-sized" training about specific topics. Education that is delivered at regular intervals and in digestible chunks builds a culture of awareness, changes user behaviors, and keeps cyber security top-of-mind for employees year round.

Consider this: If you aren't helping your employees identify the hallmarks of suspicious email and text messages, they are almost certainly putting their personal information and your systems at risk. As you weigh the benefits of effective security education, use these three tips to get on the path to risk reduction:

Think before you click – One of our customers' IT security officers told us that a targeted training goal was to have their employees pause before they interacted with a new message. "We felt that if we could gain a second or even a half of a second pause between the moment when an employee sees a link or a file and the moment when he clicks, in that gap lies the opportunity for a thought process in which the user ultimately decides, 'Maybe this isn't safe. Maybe I shouldn't do this.'" The customer gained that advantage and then some, reducing malware infections by 42% using our methodology.

Don't be afraid to follow up – A message can look and even sound legitimate but still set off a warning bell. For example, an email that comes from a corporate IT address and tells you to download new security software can seem trustworthy; it appears real and is on topic. But would that really be the process your IT department would follow? It takes just a minute to confirm a questionable message with the sender, whether it's a coworker, internal department, or financial institution.

Report suspicious messages – Fraudsters will often send the same message to hundreds or even thousands of accounts. It's not uncommon for numerous people in a company to be included in a single attack. If you suspect an email or text is malicious and is targeting corporate or personal information, report it to your IT department. This could help identify a problem early, before unsuspecting users expose themselves and your organization to dangers.

About the Author

Joe Ferrara is the President and CEO of Wombat Security Technologies. Recently Joe was a finalist for EY Entrepreneur Of The Year Western Pennsylvania and West Virginia and received a CEO of the Year award from CEO World. Joe has provided expert commentary and has spoken at numerous information security industry events including RSA Europe, the CISO Executive Network forum, ISSA International, and many regional information security conferences. His security awareness articles have been published in Network World, CSO magazine, TechWorld, FierceCIO, Computerworld, and many others.

How to move beyond the SIEM

Defending against and detecting cyber threats depends on understanding the full threat landscape

by Mark Bevilacqua, VP, Customer Success at IKANOW

Like a patrolman walking his beat, your SIEM software keeps an eye on what's happening in your network and reports any unusual activities. But just as you wouldn't rely on a security guard as the sole means of protecting your physical property, you shouldn't rely on SIEM as the sole means of providing cyber security. While SIEM provides a great deal of information, SIEM alone isn't enough to make your systems secure.

They are great at aggregating events from perimeter systems and providing a dashboard view into this information but to be truly effective in combating threats, organizations must be able to go beyond a perimeter overview. They must be able to detect and predict threats based on outside data and internal behavior across all of their systems - which SIEMs can't currently do - and a more complex data analytics platform, like IKANOW, is required to accomplish this.

Make sure you understand the capabilities and limitations of SIEM and know where you need to utilize other threat intelligence feeds and threat analytics methodologies to ensure you protect your network fully.

SIEMs focus on local & noisy data

A SIEM can capture a large amount of internal, or structured, data from multiple sources, including your network, databases, services, and applications. Years ago, this provided a fairly complete picture of your cyber posture. However, with today's dynamic, ever-changing threats, this isn't nearly good enough.

It takes time to analyze the data, and it's difficult to separate the important information from the background noise. Few firms can keep resources focused on the analysis task; there aren't enough experts to hire, even if funds were unlimited.

While automated triggers can be established, they can generate false alerts, one of the biggest complaints with SIEMs, that divert resources from important but subtle events that require a response. Tuning the SIEM to avoid generating too many false alerts may require vendor-specific knowledge that in-house teams lack. How can you make the most of this raw data?

A SIEM tells you what's going on in your network, but much security is gained by shared information. Knowing the threats experienced by other businesses lets you preemptively secure your network before hackers turn their attention to your business.

You also can't be sure that your SIEM is capturing all the interesting information within your network. Disabling monitoring and logging software is often one of the first steps intruders take once they've gained access. There's just no way to know for sure that your internal logs are capturing every interesting event in your network.

SIEMs are reactive, not proactive

By definition, SIEMs capture data about events that have already occurred. It's important to know about them to prevent them from recurring and to mitigate damage, but it's far more important to know about upcoming threats in order to prevent them from impacting your business.

Even while a SIEM captures historic data, it doesn't necessarily retain that data for a significant time — logs are often kept for only a short window. Since sophisticated attacks can extend across a long period, throwing out data after such a short time eliminates the possibility of identifying ongoing bad behavior in the network.

In addition, SIEM can only provide information about the network you already have. But network engineering is an ongoing process. Ideally, your network design changes are reviewed for security concerns before they are implemented, but SIEM won't tell you in advance if a change introduces a vulnerability.

SIEMs Provide Descriptive Data

SIEMs describe events that occurred on the network, but it doesn’t assess the impact to your business or inform you how to respond to an attack. As a result, you can't be sure you are focused on the important issues or have addressed all their impacts. Unfortunately, this missing output is really the key information you need to get value from your information security process.

Three Steps to Move Beyond the SIEM and Achieve a Complete Security Solution

There are three steps to achieving security against advanced persistent threats, in addition to implementing a SIEM.

First, both internal and external data should be captured and analyzed comprehensively and collectively; it's important to be able to integrate SIEM data with other threat intelligence feeds like iSight Partners Threatscape or Symantec Deepsight, in order to obtain a full picture of current threats. A thorough threat analytics process can correlate the disparate data sources so effectively that specific IP addresses that have been compromised can be identified.

This allows infosec leaders to quickly see where to place resources with maximum efficiency from a cost and time standpoint based on the reality of the present threats.

Second, due to the ever-increasing size of networks and the number of threats, the capture and analysis process needs to be scalable.

Scalability is pivotal so information can be utilized and the risk of ignoring a critical piece of information eliminated. The analysis needs to happen in real-time in order to be useful and allow your security team to respond quickly to current threats.

Finally, the analysis should result in actionable information (like you've never heard that term before!) that correlates directly to your network. Not all threats are equally important, and the analysis should connect hypothetical risks to specific vulnerabilities inherent in the company's network architecture.

When presented to senior leadership, the analysis should present a clear picture of the critical risks, enabling approval of the mitigation plan. When leadership and technical resources share a common view of the strategy and priorities, an efficient and cost-effective process for reducing the risks can be put in place.

About the Author

Mark Bevilacqua

As the VP of Customer Success at IKANOW, Mark is responsible for Services engagements and makes sure that our customers get the most out of their data. Mark is a veteran of the USAF and has led teams at AOL, CSC, Kastle Systems and most recently, Digital Reasoning where he helped to solve complex business data issues with advanced technology. When not spending time with his wife and two sons, he is coaching his boys in Little League and Rugby.

Register Early and Save!

Cyber Security for National Defense Symposium

Alexandria, VA | June 16-17 | Mary Gates Center




Featured Speakers Include:

Maj Gen Ed Wilson, Commander, Air Forces Cyber

Rosemary Wenchel, PDAS for Cyber Policy

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

More of the Same Won't Keep Us Safe

It's time for a reboot on our approach to network security

By Jeff Hussey, President and CEO, Tempered Networks

It is a widely understood and yet astonishing reality that all major companies have been hacked, along with countless government agencies around the world. The impact of these attacks is staggering. According a 2014 Ponemon Institute survey, the average annual cost per company of a successful cyber attack was $12.7 million. Certain industries are hit even harder, including energy and utilities companies at $13.2 million and financial services companies at $13 million. Organizations suffered an average of 1.7 successful attacks per week.

TCP/IP is the problem

How did we get to the point where cyber attacks are a routine cost of doing business? The unfortunate reality is that the Internet, specifically TCP/IP, is inherently insecure. Originally developed by the U.S. Department of Defense in the 1960s, TCP/IP was created to provide network interoperability within a closed environment of military-grade physical security. Now its purpose is to provide the backbone for wide-open, global communications and commerce. This dichotomy fuels an annual $77 billion cyber-security technology market, with no relief in sight.

Efforts to secure networks rely on encrypting communications, which requires establishing trusted relationships between the entities that are communicating. The flaw in this approach is that all of these entities are identified by their IP addresses, and IP addresses on their own assume trust. Security is typically "bolted on" after the fact, using firewalls, VLANs, VPNs, and any number of other mechanisms that cybercriminals have found ways to abuse.

Encryption is easy, trust is hard

Trust is the fundamental problem in IP communications. It turns out that adding encryption to communications is the easy part. Adding trust, on the other hand, remains an intractable problem. Why? Two reasons. First, access to apps and IPv4 communications are both tied to the same piece of information: the IP address. We do not have a cryptographic identity to use for communications, which is why we have to login to every "secure" application like banks, email, and medical records. Second, there has been no good way to manage trust relationships.

You might argue that the communications are still encrypted. But with whom are they encrypted? Does it matter if you encrypt your password over the network if goes directly to an adversary? Attribution on the Internet is nearly impossible. The browser-based trust model of hundreds of trusted CA certificates does little to assert trust and assurance for the underlying communications. Case in point is the DigiNotar CA hack.

Humans are another hurdle

To complicate matters, security is more than just a technology problem. It's also a personnel problem. A recent CompTIA survey concluded that human error is largest factor behind security breaches. Most firewalls require between 100 and 1,000 entries for configuration, and each entry is an opportunity to introduce an error. As more and more devices come online and the demand for security increases by one or two orders of magnitude, there will simply not be enough people to do the job, and existing practices will fail to keep up.

Albert Einstein famously said, "We cannot solve our problems with the same level of thinking that created them." If the root cause of Internet insecurity is the reliance on a trust-based model that is inherently insecure and can't be properly managed, how do we fix it? Ideally, we'd design a new, secure Internet that isn't based on TCP/IP, but it's too late for that. The TCP/IP ship has sailed, and we're all onboard. But make no mistake: we absolutely need a fundamental change in our approach to security.

Redefining trust

We can fix the problems associated with IP communications, by shifting the model from IP address routing to a system based on trust between cryptographic identities. At Tempered Networks, we are building the foundational elements of a secure Internet and are doing this by inserting a cryptographic identity into the communications stack: the Host Identity. This on its own only gets us so far. Orchestrating trust, at scale, between these identities is where it gets interesting. We must do this today to ensure business critical infrastructure, data, systems, and other high value assets are safe. The smart approach is to be secure by default, rather than relying on bolted-on components to become secure.

Our products are the foundational components in a defense-in-depth security architecture to provide hardened, resilient networks. Tempered Networks facilitates the provisioning and management of secure, private overlay networks over any existing network—even 3rd party networks. Each secure overlay network can be delegated to different users, while the governance of the entire solution is centralized and retained by the administrator. Effectively, it provides enterprise IT to easily deliver "Private Overlay Networks as a Service".

Elasticity through orchestration

Solving the issue of management complexity is the second critical piece of this new approach. Trust is critical, but only "automated trust" will provide the elasticity that makes it possible to configure all of these new trust relationships. The exponential growth of devices, systems, and applications converging onto IP-based networks, triggered by the Industrial Internet of Things, creates a daunting challenge for CISOs and CIOs. Effective use of all this metadata, however, can also create huge opportunities through greater business agility.

Think about the ability to harness and share real-time data about network devices, policies, status, behavior and relationships between various systems. As an example, it's common for enterprises to have hundreds or thousands of applications being accessed by employees or contractors. If the status of any particular person changes and they are no longer authorized to access applications, delays in de-provisioning unauthorized users expose businesses to risk and liability. Imagine having the ability for applications to subscribe to changes in user status. The ability to grant and revoke user access quickly and easily is critical in today's environment. Another example is theft prevention. Most organizations have high value assets that are at risk of being stolen. What if a company's building security system could quickly access information from facilities management and asset tracking systems; triggering an alarm if a high value asset is being moved off premise. The scenarios are endless with an identity-based orchestration engine that can coordinate network configuration and security policy metadata in real-time.

Playing it safe means making a change

Security is, by definition, a field that is risk-averse, which often translates into change-averse. But the state of security today is one in which we see bolted-on solutions that fail every day; at great cost to the organizations that implement them. We may still have a long way to go before we achieve a secure Internet, but we know what hasn't worked by looking behind us. As we look forward, we need to adopt a new approach in which security and automation are baked in from the start.

About the Author

Jeff Hussey has been the President and CEO of Tempered Networks since August 2014. Hussey, the founder of F5 Networks, is an accomplished entrepreneur with a proven track record in the networking and security markets. He maintains several board positions across a variety of technology, non-profit and philanthropic organizations and currently is the chairman of the board for Carena and chairman and co-owner of Ecofiltro and PuraVidaCreateGood. Hussey also serves on the board for Webaroo and the Seattle Symphony. He was the chairman of the board for Lockdown Networks, which was sold to McAfee in 2008. Hussey received a BA in Finance from SPU and an MBA from the University of Washington.

Email: j.hussey@temperednetworks.com;

Company website: www.temperednetworks.com

Jeff's LinkedIn Profile: LinkedIn

Five Username Mistakes That Can Be Worse Than Using the Same Password for All Your Online Accounts

Most Internet users are well aware that they need to be hyper-vigilant to keep their passwords and personal information protected. They have heard the recommendations that they need to use a password not related to their name, address or pet's name while including symbols, numbers and random capital letters. But, the reality is the usernames they have created for email accounts, social media and other online services could be delivering all their private details into the hands of cyber criminals – no password needed.

While it might seem harmless to include a first name and the numbers from your street address in a username, cyber criminals can harvest those details to search for other private information that you may not know is publicly available on the Internet.

"Cyber criminals use a technique called Doxing, essentially combing the web for snippets of information about a person, to build a full profile they can use to execute crimes like identity theft, scams or other targeted attacks," said Shaun Murphy, CEO of PrivateGiant. "People do not realize that if they do something as benign as posting a comment on a public page with a username like CrazyShaunOrlando those two pieces of information are enough detail for a criminal to exploit. Within minutes they can find your home address, how much you purchased your home for, what high school you attended, where your kids go to school, the list goes on."

The following five common mistakes should be avoided when creating a username, and if you are currently accessing accounts with a username that is guilty of one of these errors you will want to change it as soon as possible.

1. Recycling One Username Across Accounts – just like recycling a password is a bad idea you should avoid using the same username to log into different online accounts as well. Having one common username across accounts just makes it easier for criminals to search for and find details about your life.

2. Including All or Part of Your Name – business professionals and students often use a variation of their full name as an email address, on social media and other online forums. While people might be able to easily search for and follow or friend you, you are also making it easier for criminals to do the same.

3. Revealing Details About Your Location – whether it is the city you reside in now or where you were born including a meaningful location in your username is never a good idea. Not only

is it one more tool criminals can use to narrow their search for your personal details, it is also a common password security question.

4. Using Your Birthday or Other Meaningful Numbers – While a string of four to eight numbers might seem random a criminal will be able to use a birthday or street address to verify if the information they are accumulating is all for the same person.

5. Sharing a Username with an Email Address – linking a username with an email address can simplify a criminal's search for your personal information. Using trial and error a criminal can add common email providers to your username, run a search and pull up your social media accounts and any other sites where you have used that email address to create a profile. Some email providers including Gmail, Outlook and Yahoo allow users to alter their email address into infinite number of disposable addresses. For example if your email address is shauntips@gmail.com and you want to sign up for a new deal website you can alter your email address just for that site by adding an identifier to it such as shauntips+FreeRunningStuff@gmail.com. This keeps your actual email address private and can help stop criminals from being able to track your online history simply by searching for one of your email addresses.

About PrivateGiant

PrivateGiant is a technology firm dedicated to restoring privacy to online communications for the individual and enterprises. Its easy-to-use solutions deliver top-level security protection for text messages, emails, and messages sent or posted on social media and other public forums. PrivateGiant protects everyday communications from the moment they are sent or posted until they reach the designated recipient for decoding. Visit www.privategiant.com for additional information.

Why CISO's evolving into CBSO's should be a priority for an enterprise?

During a recent advisory session for a fortune 100 organization, security leadership walked into the conference room and proceeded to sit across the table from me. The CIO was the last individual to sit down and prior to formal introductions of his team, posed the following question to me:

"Kyle; I am a CIO as you know and I am trying to develop effective messaging to other C-Levels within my organization on the importance of hiring a CISO. What are some key points and concepts I should include in my argument to convey the necessity of a CISO, and to what extent should I employ the Fear, Uncertainty, and Doubt tactics I have heard some CIO's use to validate the need for a CISO?"

Clearly these questions were extremely important to this particular CIO and to be quite frank, I was pleasantly surprised by how direct the questions were presented and knew we could jump right into this discussion without the need for my build up slides presenting why a CISO is needed within an organization and instead discuss why they need a CBSO **more** than a CISO (essentially a CISO evolving into a CBSO).

Firstly; let's look at the two full titles of these roles:

- CISO – Chief Information Security Officer – note: the word **Information** and how this is perceived both internally and externally to organizations as an Information Technology leadership role
- CBSO – Chief Business Security Officer – note: the world **Business** and how this one word truly encapsulates all the dimensions this leadership role should have direct and or in-direct responsibility for in an organization

The business continues to view the security organization as a policy cop and a paranoid custodian that is a barrier to progress and innovation for their organization. I have spoken to a number of business leaders and board members across a number of industry verticals (non-IT business representatives) who expressed during these advisory sessions their frustration with the Information Security (IS) function. Many top executives have stated to me that they have

had poor relationships with CISO's in the past, and that unfortunately continues to shape their perceptions today. Very much like the analogy of having a bad meal at a restaurant one time and not ordering something different from the menu but instead choosing to never go to the restaurant again. These business leaders see people in the IS profession as technologists, not equals.

This translates into the number 1 compliant I hear consistently from senior business executives (COO's, CEO's, CFO's, Presidents): they are stuck dealing with very complex and technical people. This overwhelming business frustration with CISO's has resulted in a number of industry verticals establishing new, separate positions outside of IT / IS often called Chief Risk Officer or VP of IT Risk where these roles are specifically aligned with the business and their charter is to understand business requirements. Interestingly enough these roles then bring these business requirements to the CISO; who now is responsible for only for the operational execution of these requirements further dividing the chasm between IT / IS and the business. Why is this divide continuing to grow? Pretty simple answer – CISO's haven't been able to convey the following effectively to business leaders:

- ***Manage or keep pace with business demand.*** *The business and in some case other parts of information technology (shadow IT), bypass the security organization to adopt / create new business solutions only to bring their security colleagues in at the tail end of the project – prior to go-live and ask them to:*
    - *"Assume the risk" OR*
    - *"Make it secure"*
- ***A vision and focus on business innovation.*** *Hackers can compromise a ton of information in milliseconds; while at the same time the business has been very innovative in the use of technology – even "pushing" for what is often categorized as "bleeding edge" technology. Security organizations have not kept pace with these changes; in-fact, the business sees security trying to slow these changes down.*
- ***Show how ongoing operational expenditures (OPEX) and investments (CAPEX) support business activities.*** *The most critical acronym for a security executive to demonstrate to their business executive counterparts is return on security investment (ROSI). Demonstrating ROSI is a huge challenge that even top security teams struggle with quarter after quarter; year after year. This results in CIO's being incapable of outlining how their day-to-day activities are adding value to the business OR helping*

protect key corporate assets: organization reputation, customer confidence, market share, intellectual property

For the past twenty plus years I have seen the Information Security function embedded within the Information Technology discipline regardless of organization size, industry vertical, even geographic / country location. The fact remains that having Information Security embedded in the Information Technology discipline results in the role being strictly technical and often an afterthought within the organization. This type of alignment has shown to be inefficient and costly clearly pointing to business executives determining that security needs better management and leadership. This is why organizations need to help CISO's evolve into CBSO's.

The CISO is the senior-level executive responsible for establishing and maintaining proper levels of protection of **corporate assets**: *organization reputation, customer confidence, market share, intellectual property, brand protection, employee protection to name a few.* These corporate assets go beyond the traditional Information Technology discipline into all areas and processes within the organization. The trend today is for the CISO to report directly to the CIO. In order for an organization to support the CISO's evolution to a CBSO they need to have the CISO report to a senior business executive: CFO, COO, or even the CEO

If CISO's want to remain the most senior security and risk executives within their respective organizations; they will need to rethink the roles and responsibilities of the security organization, its top priorities and enterprise wide initiatives, and the services and ultimately "value" the security organization brings to the business. CISO's must also reexamine the individual skills they build within the security organization and embrace a fundamental redesign of security architecture and processes. CISO's willing to embark upon the journey of evolving into a CBSO will embrace the organizational alignment necessary to allow them to succeed. Chief Information Security Officer's need to view themselves as the Chief Business Security Officers within their organization and start their transformation today.

The keys to making the CBSO role successful are independence, empowerment, and position. The CBSO needs to be:

- Independent of influence or pressure from those affected in the protection of corporate assets

- Empowered to deploy all proper levels of protection across all areas of the organization
- Positioned within the organization to embed information security into the business culture

The CBSO should be technical but also have the acumen to provide both Information Technology, business management and business risk incisive and realistic approaches to the protection of corporate assets. The CBSO has the visibility to executive management that the information security group typically does not have except possibly during major incidents. The CBSO ensure protection schemes converge technology and business objectives with ***real*** business risk.

Key CISO to CBSO Trait Transformation examples:

- **Mentality** → CISO: Operational execution, absolute security → CBSO: Strategy, risk mitigation
- **Reputation**: → CISO: Technologist, purveyor of fear, uncertainty, and doubt → CBSO: Trusted colleague, internal consultant
- **Approach**: → CISO: Reactive, bolted-on security → CBSO: Proactive, embedded security
- **Focus**: → CISO: Security technology and point products → CBSO: Architecture, process, and analytics
- **Value Delivered**: → CISO: Operations, technology selection, efficiency → CBSO: Business enablement, support, risk mitigation

Another key methodology that CISO's must move away from is the Fear, Uncertainty, and Doubt or "FUD" methodology when interact with the business and business executives. Utilizing this methodology should not be the motivator to get executive management's attention and support for information security and its need to support a CISO within their organization.

As I asked the CIO across the table from me: If you take 100 CEO's from the top Fortune 1000 companies, put them all in a room, and ask them to very direct and candid in their response to the following questions:

- What keeps them awake at night?
- What is their most important organizational goal?

What do you think their answers would be?

The CIO and his security team looked at me and said; “to be the best in their industry – best service / best products”. My response – no. CEO’s will not say the best in their industry, nor will they say have the best technology amongst their peers, or have the best center of excellent for information security.

CEO’s will say their ultimate goal is to maximize shareholder wealth. Pretty simple.

The CBSO can ensure information security supports that goal by deploying levels of protection processes that meet actual business risk, business compliance requirements, and align to business costs.

Overall, executive management will support the CISO transforming into a CBSO and being a key member of the executive team that understands technology, information security threats and solutions that align realistically with the company’s business objectives.

About the Author

An industry leader and innovator, Kyle F. Kennedy is a Senior Executive who focuses within the areas of Information Security, Risk Management, Audit, Disaster Recovery, IT Solutions, Business Process Management (BPM), and Information Technology Governance-Risk-Compliance (GRC). Kyle is a leading expert on identity management, access management, user account provisioning, entitlement management, federation, privileged identity management, role design and management, and identity management as a Service. Kyle also covers enterprise fraud management, which has many synergies with identity and access management when an organization needs to protect against risk and wants to manage fraud appropriately.

RSA Conference 2015 Trip Report

Everything New and Innovative Under the Greatest InfoSEC Big Top

by CDM Staff on Assignment

The RSA Conference was originally launched in 1991 by and for cryptographers. Believe it or not, Cryptography is in just about everything InfoSEC from your HTTPS browsing session during an ecommerce and bank transaction to your mCommerce and mBanking on your mobile

device. Over the years it's continued to morph. One really interesting vendor we didn't see at the show but we saw recently using crypto in so many cool ways is http://www.moneyamigo.com and we expect to be doing an entire story on their innovations in the use of SMS for sending money to friends – think P2P Crypto inside your SMS. Now that's a killer app. Anyway, we digress. Back to this amazing conference. It's evolved beyond the world of crypto into anything and everything that fits into the bigger risk management equation. You need to know your threats, understand and prioritize fixing your vulnerabilities and better track and control your assets. This good old formula, R = T x V x A (Risk = Threats x Vulnerabilities x Assets) hasn't changed in many years but the solutions to fill this equation continue to evolve and the best place to find them is here at RSA Conference 2015.

By far, this conference exceeded our expectations. From a 30,000+ attendee list to an expo spilling out into two expo halls plus the Innovation Sandbox, it was nearly impossible to meet and interview all of the vendors. We decided to breeze through the isles looking for messaging about something new and exciting to catch our eye. Then we drilled down. While we recommend you see for yourself at each RSA Conference, or visiting this year's online at: http://www.rsaconference.com/events/us15 here's what we liked on the expo floor:

BAE Systems

We interviewed Jim Anderson, President – Applied Intelligence, BAE Systems and learnt about the acquisition of SilverSky, a Security-as-a-Service platform which delivers cloud-based software and managed services, such as Email Protection Services with advanced Data Loss Prevention, Targeted Attack Protection, Network Security Services, and Managed Application Services that protect critical information simply and cost effectively. SilverSky's highly skilled sales, marketing and engineering workforce and experienced management team will join Applied Intelligence's Commercial Solutions division. Visit them online at http://www.baesystems.com/

Daon

We were introduced to the Daon IdentityX Platform which allows organizations to mix and match entire security systems into their overall security schema, which includes the IdentityX Authenticator, legacy systems such as RSA tokens, Active Directory password systems and new emerging device capabilities such as mobile phones with embedded fingerprint readers. Daon's IdentityX Mobile Biometrics Solution makes use of Facial Authentication with Liveness, Voice Recognition and PIN verification. This triumvirate of Face, Voice and PIN options allows users to select their desired means of identity verification based on the circumstance at the moment. Visit them online at http://www.daon.com/

Grier Forensics

Jonathan Grier of Grier Forensics educated us about the dangers of malware hidden in Microsoft Office documents which can be used to exploit devices and networks resulting in costly data breaches, cyber espionage and more. Microsoft Office is the preferred choice for hackers because of its popularity, and the fact that it is almost an OS in terms of functionality. He explained that each page of a document comprises of parts and every part has a content types and relationships. Documents can be dissected using the OfficeDissector tool which can be found here (http://www.officedissector.com/) and the tutorial can be found here (http://www.officedissector.com/doc/rst/ANALYZING_OOXML.html). Visit them online at http://www.grierforensics.com/

Nuro Secure Messaging

Nuro Secure Messaging is a cognitive enterprise-grade secure group-messaging platform designed for employees and external trusted partners to communicate in a controlled and compliant private messaging environment. Over 3 billion people use instant messaging and that is Nuro's target market. They have four layers of security: at the user's device, encryption during transit, encryption at rest, and cognitive security that predicts breaches. Nuro can be deployed as a SaaS solution or on-premises for complete control. It offers cross-platform support and APIs for deployment in any IT environment along with white labeling. Visit them online at http://nuro.im/

Bluebox

Bluebox transforms your everyday commercially available mobile app into a secure mobile app in minutes with no coding or SDK required. Bluebox protected apps can detect and defend itself against mobile threats and respond immediately to attacks to prevent mobile breaches. IT Managers can gain actionable insights from app behavior, threat behavior and adapt security policies to reduce risk and protect corporate data. Visit them online at https://bluebox.com/

Cybertinel

We found CYBERTINEL's endpoint security platform to be a signature-less security solution, which combines multi-layer data collection, through lightweight agents, with central analysis using five powerful analysis engines. Through its deep analysis and wide perspective, Cybertinel is able to discover the attacks' source, behavior, strategy, history and creators, while providing immediate remedies and countermeasures. Visit them online at https://cybertinel.com/

Malwarebytes

Malwarebytes Anti-Malware for Business reduces your vulnerability to zero-hour malware, including ransomware, by delivering industry-leading detection and remediation. Their proprietary blend of heuristic and definitions-based technologies protects against these threats at zero hour, including ransomware and if your endpoint security fails to detect malware, Malwarebytes award-winning remediation technology will remove it completely. The platform has a small system footprint and enables IT Managers to create policies based on user groups and aggregates threat data. Visit them online at https://www.malwarebytes.org/

Agari

Agari Email Trust Cloud secures your email channel against cyberattacks. It makes it possible for enterprises to secure their employee and partner community from the threat of business disruption and data breach in turn safeguard sensitive customer data that can be used to hijack legitimate, personalized consumer email marketing campaigns that in turn hijack customers' systems and disrupt real lives. Agari Email Trust Cloud empowers enterprises to have authentic online relationships and create a trusted ecosystem. Agari Enterprise Protect uses trust as a medium to authorize and verify authentic inbound emails, Enterprise Protect can block targeted spear phishing emails & can prevent cybercriminals from establishing a beachhead for a broader data breach and ensure that the only emails your employees get, are the ones they can trust. Visit them online at http://agari.com/

Interset

Interset utilizes behavioral analytics, machine learning, big data and risk forensics to provide a highly intelligent and accurate insider threat and targeted outsider threat detection solution. Weighted risk scores are assigned to people, devices and data assets. These risk scores change as events occur and literally connect the dots of events that are threats to your sensitive data. Interset detects these anomalous and high risk events and prioritizes them. Visit them online at https://www.interset.com/

Whitecryption

WhiteCryption's enterprise solution, Cryptanium, offers two security components: Secure Key Box and Code Protection. Secure Key Box is a state-of-the-art white-box cryptography that keeps secret cryptographic keys well hidden within app code even during runtime and Code Protection is a tool used to "harden" software application code to prevent reverse engineering and other techniques used by cyber-criminals to gain access to sensitive information and resources contained in applications. Visit them online at http://www.whitecryption.com/

In Conclusion

On behalf of Cyber Defense Magazine, a Platinum RSA Conference Media Sponsor, we must say "kudos" to those who won awards from us during the conference and to those (above) we found in the expo hall. The innovation each year is astounding. It's up to you to decide which one of these solutions best fits your needs. Use the risk formula, choose something one step ahead of the next threat or vulnerability or BYOD (bring your own device) dilemma and you'll be happy you spent time at RSA. Don't forget, the Expo is just the tip of the iceberg. If you take a look at all the speakers and topics, you'll find only the top shelf of the INFOSEC industry. If you didn't make it to RSA Conference 2015, keep an eye on this website and find your way to their next event: https://www.rsaconference.com/ like London next week or Singapore in July or Abu Dabi in November.

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

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?

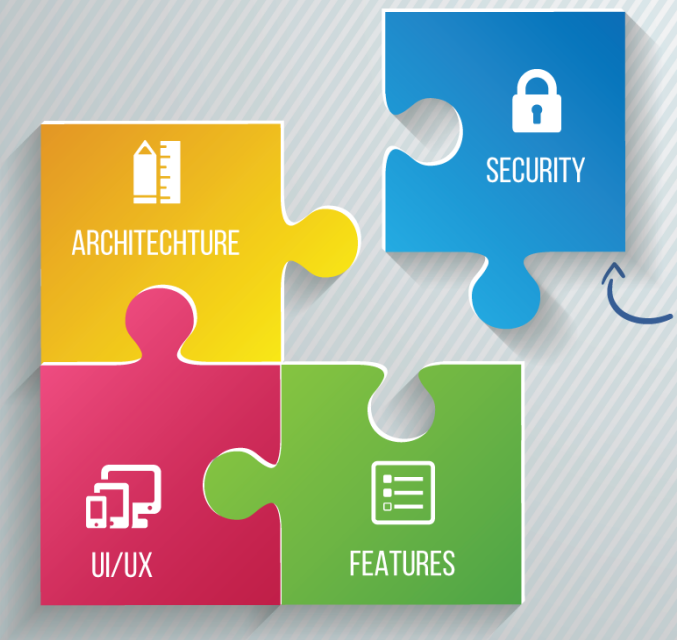
Your Enrollment includes :

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.

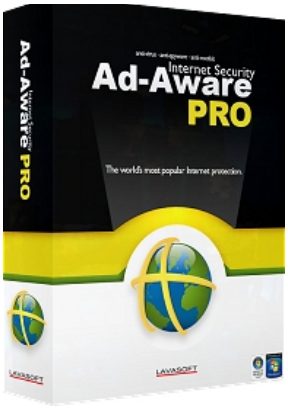
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting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

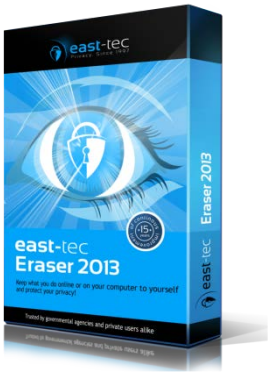
Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

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

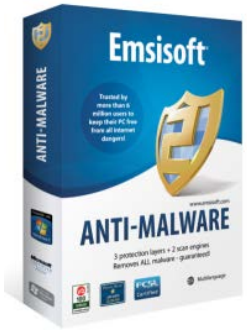
SOURCES: CDM and NAISG.ORG





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 May 2015

Sample Sponsors:

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

Cyber Warnings Newsflash for May 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…

Ryanair falls victim to €4.6m hacking scam via Chinese bank

https://www.irishtimes.com/news/crime-and-law/ryanair-falls-victim-to-4-6m-hacking-scam-via-chinese-bank-1.2192444

Harbortouch is Latest POS Vendor Breach

http://krebsonsecurity.com/2015/05/harbortouch-is-latest-pos-vendor-breach/

How the Pentagon Could Soon Share Americans' Data With Foreign Militaries

http://www.defenseone.com/technology/2015/04/how-pentagon-could-soon-share-americans-data-with-foreign-militaries/111553/

Hard Rock Hotel & Casino suffers data breach

http://www.csoonline.com/article/2917674/data-breach/hard-rock-hotel-and-casino-suffers-data-breach.html

Lawmakers criticize FBI's request for encryption back doors

http://www.computerworld.com/article/2916895/encryption/lawmakers-criticize-fbis-request-for-encryption-back-doors.html

What Walmart Learned From the Target Data Breach

http://www.eweek.com/security/what-walmart-learned-from-the-target-data-breach.html

Mixed Verdicts in Second Trial of Aleynikov, Ex-Goldman Sachs Programmer

http://www.nytimes.com/2015/05/02/business/dealbook/ex-goldman-programmer-found-guilty.html

More Uber Accounts Have Been Hacked, This Time in the United States

http://motherboard.vice.com/en_uk/read/more-uber-accounts-have-been-hacked-this-time-in-the-united-states

How fear and self-preservation are driving a cyber arms race

http://www.cnet.com/news/how-fear-and-self-preservation-are-driving-a-cyber-arms-race/

Foiling Pump Skimmers With GPS

http://krebsonsecurity.com/2015/05/foiling-pump-skimmers-with-gps/

VA Blocked Billions of Cyber Threats in March

http://www.defenseone.com/technology/2015/05/va-blocked-billions-cyber-threats-march/111721/

Windows XP support deal not renewed by government, leaves PCs open to attack

http://www.v3.co.uk/v3-uk/news/2406304/windows-xp-government-support-deal-ends-leaving-pcs-open-to-attack

Lets Call Stunt Hacking What it is, Media Whoring.

http://carnal0wnage.attackresearch.com/2015/05/normal-0-false-false-false-en-us-x-none.html

First Example Of SAP Breach Surfaces

http://www.darkreading.com/attacks-breaches/first-example-of-sap-breach-surfaces/d/d-id/1320382

Strategic Friendship in Asymmetric Domain

http://www.pircenter.org/en/blog/view/id/208

Someone Hacked a Billboard in Atlanta to Display Goatse

http://motherboard.vice.com/read/someone-hacked-a-billboard-in-atlanta-to-display-goatse

GCHQ spies given immunity from anti-hacking laws

http://www.telegraph.co.uk/technology/internet-security/11612659/GCHQ-spies-given-immunity-from-anti-hacking-laws.html

Feds Say That Banned Researcher Commandeered a Plane

http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

Industry cyber info-sharing body to launch new 'ISAO' for insurers

http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/industry-cyber-info-sharing-body-to-launch-new-isao-for-insurers/menu-id-1089.html

Korean Log-in Security Questions 'Too Easy'

http://english.chosun.com/site/data/html_dir/2015/05/22/2015052201606.html

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

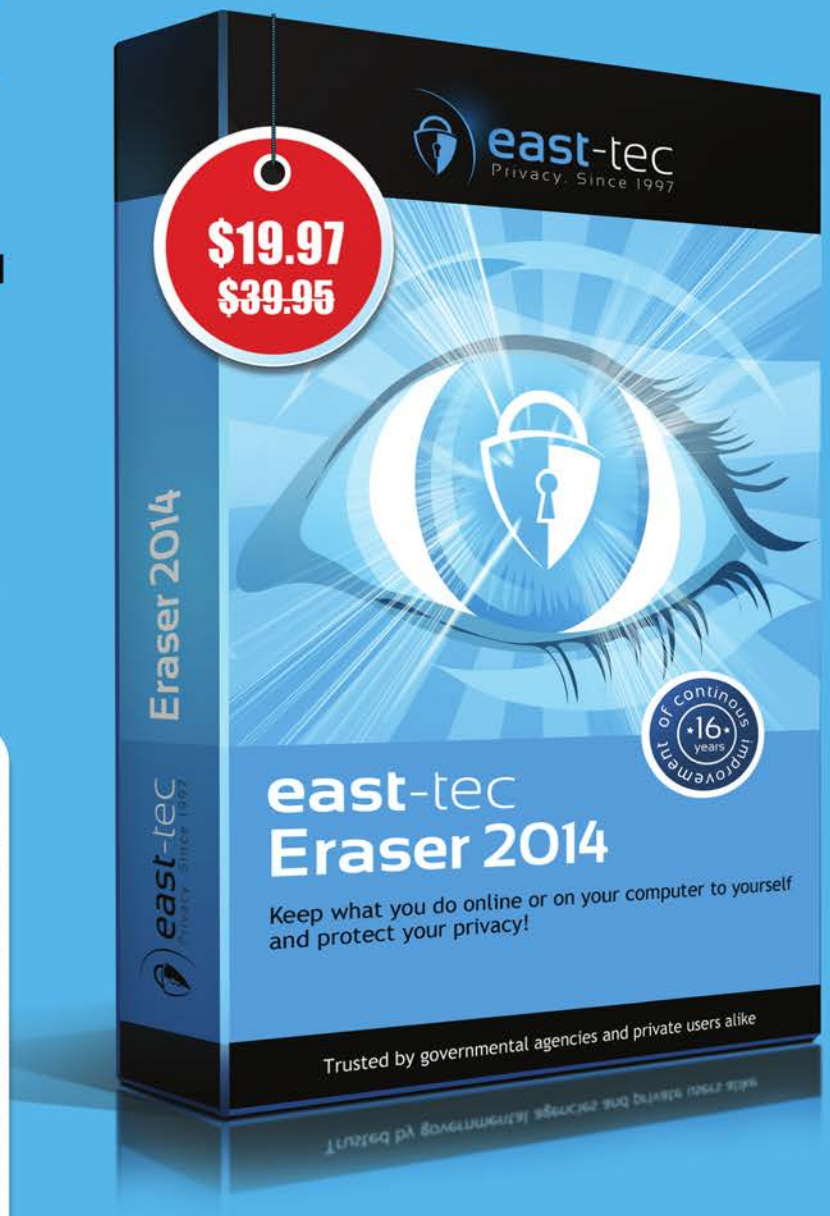
Cyber Defense Magazine - Cyber Warnings rev. date: 05/27/2015

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