CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

FEBRUARY 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

Nish Modi
Anna Wehberg
Todd Weller
Chris Rouland
Justin Rogers
Chris LaPoint
Milica Djekic
Kyle F. Kennedy
Mike Miranda
Artin Amirian
Robert Neivert
Scott Schweitzer
Stuart McCafferty
Edwin Covert
Andrew Blaich
Gunjan Tripathi
Gary Miliefsky
Dean Wiech

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®

Data Breaches – a Common Theme? Spear Phishing & RATs

It all started with the mainstream media covering the Sony Pictures Entertainment breach (SPE) – the debates about who did it – Chinese, Russians, North Korean government, etc. What was missing from this debate started to become even more clear as we saw the Anthem breach of 80,000,000 records of Americans – their entire PII file – name, address, date of birth, social security number, salary range, home phone, mobile phone, email and much more. Then, as I covered online, the major breach of 100 banks which totaled over $300M (Kaspersky says it will hit $1B) in banking fraud/theft/money laundering.

This again brought us to one simple conclusion – the process of network mail protocol reconnaissance followed by targeted spear phishing attacks that include zero-day or new remote access Trojans (RATs). It's a repeat story that I expect we will see over and over, especially in America and Europe, where companies who think their firewall and antivirus technologies are sufficient forget the most important factor – people. They don't train them well when it comes to best practices for Information Security (INFOSEC). If they did, defenses against phishing attacks and understanding RATs would be first on their list.

We hear over and over 'it was too sophisticated for us to detect'. This common theme is a common excuse that won't work when law suit after law suit and fines from government agencies pile up because these companies that we entrust our private information to, have no clue about proper INFOSEC training and the most simple of countermeasures – defense against phishing attacks.

We can add the bring your own device (BYOD) dilemma to the equation – I would think many of these mobile devices are also infected with RATs. What this means is – SMS messages, emails and untrustworthy app downloads are where the cybercriminals minds are at but most businesses and consumers are not. Time to think about this and become a bit more proactive. So in this month's edition we have great writers covering subjects including Security Automation, Internet Of Things, Data Breaches, Damage Control Tips and of course the big area of risk - Mobile Device Security. Stay vigilant – stay one step ahead of the next threat.

To our faithful readers, Enjoy

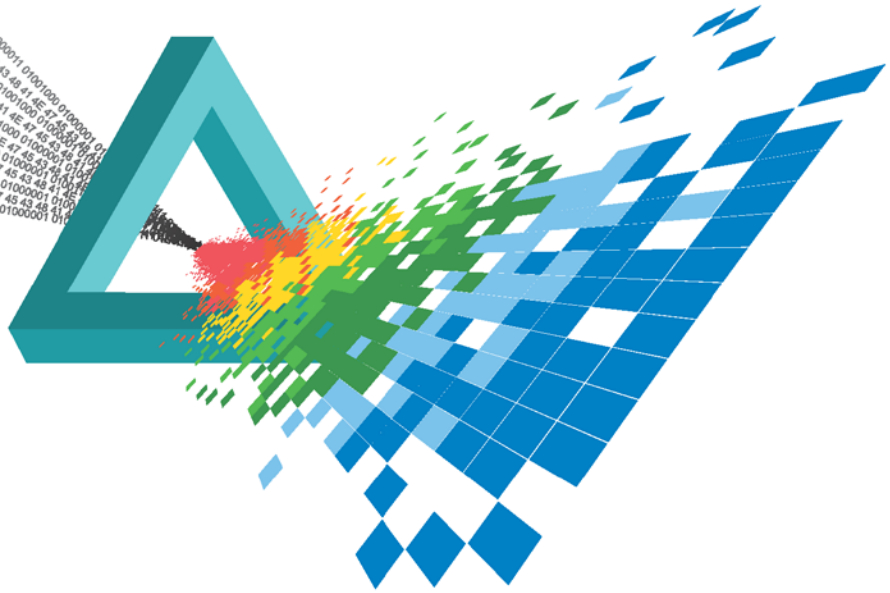
Pierluigi Paganini

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

RSA Conference 2015

San Francisco | April 20-24 | Moscone Center

Save $400 on your Full Conference Pass
during the Discount Period
Discount ends March 20



CHANGE

Challenge today's security thinking

Register now for RSA® Conference 2015

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

- **23 tracks**—including 3 new ones!
- **350+ Sessions**
- **400+ Exhibitors**

Experience these exciting programs:

- **RSAC Innovation Sandbox**
- Live streaming video on **RSAC TV**
- Great lineup of **Keynote speakers**

Guest Keynote Speaker
DIANA NYAD
World Record Holder
and Legendary Swimmer

FOLLOW US ON: #RSAC

Register Now! **www.rsaconference.com/cdm**

DIAMOND SPONSORS

intel Security · Microsoft · RSA

PLATINUM SPONSORS

ca technologies · cisco · hp · JUNIPER NETWORKS · QUALYS Continuous Security · Symantec.

PLATINUM MEDIA SPONSOR

CDM Cyber Defense Magazine

The New 3D Secure – Too Little, Too Late?

By Nish Modi, SVP of Product & Innovation, SecureNet

When 3D Secure was first announced by Visa, it promised to add an additional, much-needed layer of security to debit and credit transactions. Financial authorization is paired with online authentication through a series of three domains: the acquirer (the merchant), the issuer (the bank) and interoperability (the infrastructure used to support 3D Secure). The protocol was, however, quickly condemned for increasing phishing scams. Now, EMVCo has announced it will take over the development of the next version of this technology – but is it too little, too late?

Weak Spots

The current 3D Secure solution is clunky at best, and the consumer experience is less than ideal. Users are still required to authenticate themselves via their issuer using a PIN or passcode before they can complete the purchase.

For merchants, 3D Secure is expensive to deploy. Considering the low issuer participation, the cost does not justify the consumers that will be validated through this solution. Moreover, not all issuers in the U.S. – like Citibank and Chase – participate in 3D Secure, so for many merchants the benefits do not justify the cost. This is just one of the many reasons why 3D Secure never really gained any traction in the U.S. Even in other parts of the world where 3D Secure has been implemented, such as the European Union, 3D Secure was deployed because of government mandates. Perhaps most importantly, in this day and age of mobile and in-app payments, the current 3D Secure does not adequately factor in and address changing consumer shopping behavior.

Potential Pitfalls

So will the new 3D Secure be any better? EMVCo promises a more intuitive consumer experience coupled with intelligence-based risk monitoring and decision making services that place less of a burden on the cardholder to verify the transaction. It also promises to streamline country-specific regulatory requirements that currently put global merchants processing international payments with 3D Secure at a significant disadvantage.

Though these improvements sound promising, there are several critical weak spots in the current solution that the new solution does not address. There are still major financial institutions, specifically in North America, that have not and likely will not participate in 3D Secure. What's more, by the time the new technology is developed and deployed, there are other payments security solutions that will have become far more advanced and widespread.

Alternative Technologies

Continued improvements upon and progress in various payments solutions will soon make both the new and old 3D Secure irrelevant. Changes in encryption technology, for example, are guaranteeing zero exposure of plain text, non-encrypted information on the part of the merchant. Specifically, tokenizing pre-authorized transactions allows users to register their payment methods with the processor's secure vault. Customers' sensitive card data therefore never touches the

retailers' servers, a critical advancement when considering that most well-known retail data breaches (like that on Target) have taken place at the merchant server level.

Additionally, enhancements to network tokenization support are expanding into e-Commerce, protecting consumer and card data for the transactions initiated online or via mobile devices.

Finally, biometric payments are going to take center stage in 2015. ATMS are expected to adopt biometric authentication and Visa and MasterCard plan to replace their online password systems with biometric technology later this year. With Apple Pay consumers are already using fingerprint ID to make purchases. The implications for a higher form of security are certainly clear with biometrics, with the added benefits of ease of use and convenience that in many ways 3D Secure cannot offer.

While developments in the new 3D Secure are one to watch, it's important to consider all of the weak spots in the existing solution – poor user experience, cost, lack of participation – that need to be answered in the new proposed solution. While some advancements to the protocol – such as more intelligent risk monitoring and globalized integration standards – are underway, alternative technologies will quickly surpass 3D Secure by the time it is ready to be deployed on a wider scale. When considering the rate at which breakthrough technologies like biometrics are hitting the market, one can't help but wonder if the new 3D Secure will be too little, too late.

About the Author

Nish Modi is the SVP of Product and Innovation at SecureNet, and end-to-end payment processor headquartered in Austin. He has more than 17 years of industry experience. To learn more about SecureNet and get in touch with Nish, visit www.securenet.com.

Cybersecurity Q&A with Fran Howarth, senior analyst at Bloor

By Anna Wehberg, Sr. Marketing Director, Hexis Cyber Solutions

In January, Hexis hosted the 2015 EMEA Exchange conference in London, which consisted of two days of cybersecurity workshops, discussions and networking. We sat down with keynote speaker and Bloor senior analyst, Fran Howarth, to chat cybersecurity, and this is what she had to say:

Hexis: *What do you see as the biggest cyber security threats facing companies today?*

Fran Howarth: The biggest cybersecurity threats facing companies today revolves around the increasing complexity of networks, relative to the connected number of users, applications and devices. As we move into the Internet of Things, we'll find ourselves immersed in a tangled web of complexity – the only way we'll be able to make sense of these types of convoluted environments is by prioritizing the monitoring of our endpoints.

Advanced cyber attackers are identifying new ways to penetrate our networks – through the endpoint. As a result, a call to security experts has been made for the development of solutions that protect and monitor the endpoint. Through continuous monitoring and continuous response of malware attacking the endpoint, security professionals will be able to better sort through false positives and address high-priority attacks.

Hexis: *When you speak to security professionals at end-user companies, what is their general security outlook?*

Fran Howarth: Security professionals at end-user companies are aware of the existing issues related to security in today's complex environment. In these instances, the sad truth is that many organizations still view security strategies and precautionary measures as a bottleneck rather than as a priority.

Fortunately, for the remaining companies, there is a slow, but increasing level of awareness that security is important. For these organizations, we've seen the steps taken to create and foster a culture that stresses the importance of security.

The biggest problem that we're facing today, however, is the lack of skilled IT security workers. There is an issue with resources and it's becoming more and more evident as we realize that responding to every single threat is impossible.

One solution to this problem is directly tied to automation. By continuously monitoring and remediating endpoints across an organization, the likelihood of an impending breach becomes smaller and smaller. Automation is a critical aspect of the incident response strategy.

Hexis: *What are security teams at your customer sites doing right? Where have they made mistakes and how do you advise on alternative security strategies?*

Fran Howarth: Companies have recognized that it's no longer a matter of just preventing but rather detecting. This proactive strategy lends itself to the tried and true mantra of "It's no longer a matter of if…but when you'll get attacked." The companies that understand it's only a matter of time before they fall victim to a breach, are in a better position than those that are still leveraging legacy solutions such as anti-virus and firewall technologies. Continuous incident response and continuous incident remediation are proactive strategies that companies across all industries must fully understand.

About the Author

Anna Wehberg, Sr. Marketing Director, joined Hexis Cyber Solutions in April 2014.

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

American Conference Institute's 10th National Advanced Forum on

CYBER & DATA RISK INSURANCE

Discount Code: CDM200

Coverage, Underwriting and Claims Strategies for Managing Privacy/Security, Data and Network Risk and Liability

March 23–24, 2015 | Fairmont Chicago Millennium Park Hotel | Chicago, IL

Featured Speakers From:

SEC
FTC
FBI
US Attorney's Office (CA)
Virginia AG's Office
Massachusetts OCABR
Texas OAG Consumer Protection Div.
Conn. Dept. of Consumer Protection
Pa. Office of AG, Bureau of Consumer Protection
Missouri AG Office
Florida Office of the AG
Markel
Zurich
ACE
Argo PRO
AIG
Endurance
Socius Insurance
Euclid Managers
The Hartford

Conference Co-Chairs

Kirstin Simonson
The Travelers Companies, Inc.

Richard J. Bortnick
Traub Lieberman Straus & Shrewsberry LLP

Featuring Key Insights and Expert Advice on:

- **Federal regulatory, legislative, and enforcement landscape:** changes on the horizon and integrating new and anticipated initiatives into your practice
- **View from the states:** emerging regulatory and enforcement activities and the growing authority of the state AG offices for breaches and failure to notify
- **State of the market** for first- and third-party coverage and losses: **new underwriting issues** in a connected world and with highly exposed industries, today's **key considerations for brokers and carriers,** and the **latest on coverage arising out of sensitive data breaches, new technologies and more**
- **Credit/debit/payment card security and the insurability of large retailers:** credit card exploitation; security procedures to prevent/mitigate hacking, theft, and security breaches; chip and pin technology; and issues associated with **PCI compliance**
- Spotlight on **data breaches for financial institutions**
- Emerging perils, new risks, and **cyber crime eclipsing terrorism as the principal domestic threat**
- **Healthcare provider/health insurer data breaches** and liability implications of a loss of protected health information
- **Business abroad: conflicting security and compliance obligations** in and across varying jurisdictions, **trends in international claims for cyber attacks and breaches,** and market conditions and cyber insurance product availability outside of the U.S.
- **Cyber liability class actions & litigation** and their impact on assessing what breaches and resulting claims are worth: latest on standing; recovery of costs for breach recovery efforts and coverage for actions for cybersecurity preparedness

Sponsored by: AllClear ID ALERT NETWORK

as well as:

Hartford Steam Boiler
CRC Insurance Services, Inc.
QBE North America
OneBeacon Technology Insurance
Chubb Group of Insurance Companies
Axis Capital
Beazley Group
Marsh
Swiss Re
Allied World
Liberty International Underwriters
Western World Insurance
Wells Fargo Insurance
HUB International
Travelers
Crum & Forster

Earn CLE Credits

Earn CPE Credits

Be sure to also book for Workshops A and B:

A The Fundamentals of Cyber & Data Risk Coverage

B Negotiating and Drafting Cyber Risk Provisions and Policies

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

Why automated incident response should be on your next boardroom agenda

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

After the year-long streak of high-profile cyberattacks in 2014, enterprise network security is no longer just about IT. More than ever before, cybersecurity is coming into the focus of boardrooms in just about every industry. Having seen the legal and reputational nightmares that Sony, Target and other large enterprises had to face, board-level executives are on notice and looking for ways to avoid being next in line for a crippling cyberattack.

Where are enterprises directing their investments in cybersecurity?

It's no longer a matter of if a business will be attacked, but when. That may be why a recent survey from the Ponemon Institute found that the majority of enterprises are investing more into incident response, rather than solely in traditional perimeter-based defenses.

More than 55 percent of the Ponemon's survey respondents said that the public's increased awareness of cyberattacks was a key reason why they built incident response teams to help stop an in-process attack. Detection, a necessary precursor to response, is also growing in prominence. In particular, continuous, automated detection is becoming essential to finding threats and alerting the response team as soon as possible.

Why the response team might not be enough anymore

Having trained professionals at the helm is certainly a necessity in cybersecurity today, but given the evolution of the threat landscape, comprehensive network security may require more than just a human touch. Nowhere is this more pronounced than in the health care industry, which faces higher risks and greater costs in the event of a cyberattack than any other industry.

According to a recent article from Government Health IT, attacks are becoming more frequent and complex. In addition, regulators have imposed even stricter standards for reporting, which has led health IT security teams to respond to incidents at a higher rate than ever before. At some point though, this will become unsustainable - an organization can't just keep throwing more people at the problem and expect to contain costs.

As the news source noted, when attacks are happening so often and in such a high volume, enterprises need to find response tools that scale. Fortunately, there are automated detection and removal tools that catch attacks and deal with them as fast as they come. Adopting these tools will allow enterprises to remain effective no matter how often hackers try to break in, while keeping human capital costs down.

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

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

As Data Proliferates in the Internet of Things, So Does Risk

By Chris Rouland, Founder and CEO, Bastille

Consumers don't read privacy policies. While this isn't news, a recent PEW Research survey showed that more than half of Americans don't even know what a privacy policy really is. Many consumers cite the length of privacy policies as a reason for not being informed, but few realize the implications that could result from this negligence.

So how much do people really understand about what it is that they're giving up when they buy an Internet connected device? Take, for instance, "smart" TVs. These televisions take home entertainment to the next level, giving owners not just amazing visuals, but also the ability to use things like voice recognition to change the channel or turn up the volume. This seems like a revolution for those of us that seem to always be misplacing the remote, but there is a down side to being able to talk to your TV.

I dug into one popular manufacturers privacy policy and we were alarmed at what we saw. According to the Samsung Smart TV Addendum in their privacy policy, Samsung may send your voice data "to a third-party service that converts speech to text". This seems innocuous enough; after all, we are accustomed to applications using our historical preferences to serve up more relevant ads and information. However, Samsung's policy goes on to read, "please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

Wait a minute. I'm okay with Samsung knowing that I spent the weekend catching up on *Homeland,* but capturing personal conversations that I have in the comfort of my living room? This is a true invasion of our most intimate spaces and cannot be tolerated.

While it may seem I'm picking on Samsung, I actually applaud them for being so plain spoken (I bet they pick a sneakier law firm for their next EULA). Most of the other electronics companies make their privacy policies so complicated you need a lawyer to make sense of it. For those that don't require you to have a JD to understand it, they're so vague and ambiguous that it's almost a waste of time to read. And time is another factor dissuading consumers from being informed. The average privacy policy takes 10 minutes to read. And, the average American encounters nearly 1,500 of these policies per year!

Many of us are okay with releasing some of our private habits to our technology provider; after all it's much better to be served advertisements for things we actually want. But having our personal conversations analyzed so that corporations know about our most intimate affairs is going too far. Imagine that you're discussing your upcoming surgery over a meal and you turn on your TV to be greeted with an ad for life insurance.

When Privacy Becomes Security

Samsung is transmitting your data through pretty normal means, the Internet, either wired or wireless, protected by your ISP. But "smart devices" are becoming a norm and many of these are designed to go with you. As such, battery life is a concern. To address that, manufacturers are relying on newer protocols such as Bluetooth LE (low energy) and ZigBee. In turn, these protocols

create a personal area network (PAN), which is allows each person to use a mobile device as a networking hub. What you end up with is a lot of data transmitting across a lot of devices using a lot of different protocols.

And…lots of opportunities for that data to be intercepted.

The World Economic Forum released its Global Risk Report which states that IoT hacking is 'very likely' and points out that today's Internet infrastructure was simply not created to handle this kind of flood of new devices. CES2015 also reinforced this sentiment, with FTC chairwoman Edith Ramirez warning that attackers could "access and misuse personal information collected and transmitted by [IoT] devices." While Smart TV's have access to a fairly safe means of transmission via Wi-Fi or hard-wired Ethernet, the market for IoT devices is growing by the day. These devices have equally loose privacy policies and are constantly sharing data between devices and apps; all of this activity is putting data at risk for exploit.

Another example of this data dragnet is Uber, the car service that has made transportation a socially connected service. No more hailing a cab, now you simply request an Uber driver from your phone. Uber made the news late last year for it's questionable data collection. While, sure, it needs your geolocation to send a car, it also take the opportunity to look at your contacts, your geolocation *history*, what apps you have installed – even your neighbor's Wi-Fi information. The list is endless and has nothing to do with a car service. It's clear that data is a secondary business for Uber. And, looking at their privacy policy - that you agree to in order to use the service – they are able to share it. This means *your* data drifting around the Ethernet to third parties that that may "perform other administrative services". Whatever the hell that means.

For certain, data analytics is big business. But, this is your data that is flying around out there. As it makes it's stops between your service provider and whatever third, fourth, or fifth parties their sending it to, this data as more opportunity than ever to intercepted and captured or for your personal area network devices to be compromised.

Read your privacy policies. It will be up to each of us to determine what we're willing to give up in the name of modern convenience.

About the Author

Chris Rouland is a cybersecurity expert and entrepreneur. He is currently the founder and CEO of Bastille, the first company to detect and mitigate threats to the Internet of Things.

Time is not on your side.

The threat landscape is forever expanding and adapting. With millions of malicious users hiding amongst billions of legitimate users, it is no wonder that cyber attacks are consistently at the forefront of every major news station.

Cyber security systems must be able to meet the breadth of today's attacks. Without this sort of scalable solution in place, the next breach could be right around the corner.

One of the biggest issues in cyber security today is the widening time gap between an adversary's ability to breach a network, and the security team's ability to discover that breach.

The threat landscape is a dynamic attack surface; keeping up with the changes is proving to be a losing strategy. Adversaries are taking advantage of the slow speeds in which a security team is able to respond to the attacks.

According to the Verizon Data Breach Investigations Report (DBIR), as many as 90% of reported breaches occur within "a few days." These breaches can take all forms, from spear phishing and social engineering, to exploits and tampering. It's getting easier and easier to check new malware against the existing signature databases to ensure that the latest attack won't be immediately detected.

Malware is even being developed to detect that it's being run in a virtual environment, and not disclose it's true intent.

With the same criteria of within "a few days," the DBIR report indicates that security teams are able to discover only 30% of breaches. In an ideal world, security teams would discover a breach within seconds of it occurring, enabling the fastest response possible to the incident, preventing a compromise from becoming a crisis.

In reality, it takes days, weeks, and even months to discover these breaches, ranging in severity from fairly benign to state-sponsored Advanced Persistent Threats (APTs). Likely, there are breaches in enterprise networks that persist for years, completely undetected.

How will the tables be turned? Is it possible to close this gap?

In most enterprises today, security teams are designed to take on these challenges. This is a monumental job, and there are varying levels of success throughout the industry. Logistical problems, such as geographic location, have to be factored in.

What if there isn't enough security talent in my location to be able to bring in the best? Technology problems will continue to evolve. What if we experience a breach the likes of which nobody has ever seen before? There is no user manual for dealing with these new emerging threats.

Cyber Threat Visibility is essential to closing the breach detection gap. It's not an option for a small team with this monumental task to work on their own in a vacuum. Organizations focused on the research of these threats are growing.

Specializing in market verticals, attack vectors, and even tracking threat actor groups, these intelligence companies are tracking the worst of the worst across the industry today. It's essential in today's threat landscape for security teams to augment their capabilities with cyber threat intelligence.

Leveraging this knowledge on the enterprise enables organizations to know what to look for or sometimes simply, where to look, speeding up incident response.

Implementing this research makes security teams more effective, focusing on actionable threat data. This reduction in false-positives will reduce an organization's overall risk, as they are aware of potential compromise events faster than ever.

There's still another gap.

Knowing about a breach and having the capabilities to fix it are not one in the same. Cyber threat intelligence is a tremendously powerful resource. Many of the providers and on-site security teams that are generating intelligence have the ability to communicate the issues and strategies for taking action against the matching events.

Again, sharing this information, and being able to communicate as close to the breach event as possible is critical for protection, but there's still a gap, the detection to protection gap.

Most of the largest retail breaches that we have seen occur at times when teams are least prepared to engage and take action. Before Thanksgiving until mid-January, financial transactions among retail and online stores are never higher.

Companies want to be able to collect and process payment for all the shoppers, and they don't want mistakes or human error to take these systems offline for any period of time. The loss of revenue for even an hour can be disastrous. To avoid human error, freezing configurations and systems in place is fairly standard across the industry.

What happens when the adversary knows this, and exploits this timing for their gain? Unfortunately, it happens all too often. Even when threats are identified during these freeze windows, taking corrective action is often too late to have a meaningful impact.

In order to solve these challenges and effectively implement cyber threat intelligence in the network security stack, new technologies must be deployed for real-time identification and protection of network resources.

These new capabilities must be able to handle the large, dynamic policies specific to their industry, and identify the potential compromise down to the exact internal resource. The cyber threat

visibilities gained from these new technologies are vital in securing data and keeping organizations' networks safe from attacks.

About the Author

Justin Rogers, Director of Product Marketing
Centripetal Networks

Justin has more than 15 years of experience in networking, telecommunications, and the defense and intelligence communities. Justin previously spent several years with the Combined Explosives eXploitation Cell (CEXC) deployed with a joint-expeditionary team in Baghdad, Iraq, as well as Bagram, Afghanistan. With CEXC, Justin focused on Counter-IED technologies, training, and bridging the protection gap in defense of Coalition Forces. After joining Centripetal Networks in 2012, Justin has been focused on bringing Centripetal's Active Network Defense platform to market. Justin has a BS in Electrical Engineering from the University of New Hampshire.

FT
FINANCIAL TIMES

FT CYBER SECURITY SUMMIT USA 2015

Protecting businesses in cyberspace

March 18, 2015 | 10 on the Park **NEW YORK**

FT Cyber Security Summit USA will build on and extend the discussions at the inaugural Summit in London, with a sharper focus on the threats facing businesses, especially those in critical national infrastructure industries such as financial services, energy and transportation.

The Summit will bring together executive managers, corporate information security officers, consultants and IT vendors to discuss the broader business issues of cyber security. It will also feature top officials from government departments and agencies who have responsibility for developing national cyber security strategies that help both the public and private sectors manage existing and emerging cyber risks.

For more information about the conference, please contact Chrissy McNasby:
+1 917-551-5101 or **chrissy.mcnasby@ft.com**

For sponsorship opportunities, please contact Toufique Khan:
+44 (0) 20 7873 3260 or **toufique.khan@ft.com**

@FTLiveDigital #FTcyber

IT Pros Beware: The Security Risks of Shadow IPv6

By Chris LaPoint, Vice President, Product Management, SolarWinds

The impending transition from IPv4 to IPv6 has been an ongoing discussion for years—the Internet is running out of IPv4 addresses, IPv4 isn't "future-proof," IPv6 will make managing networking services much easier, and so on. However, despite the buzz, IPv6 addresses still make up just four percent of today's Internet. And adoption will likely continue to be slow—mostly due to costs associated with making the switch.

However, IT pros should not be fooled by this, as it's highly likely IPv6 is already enabled and operational in many organizations whether they know it or not, creating "shadow networks" of unmanaged IPv6-enabled devices that can pose significant security risks. So, the question is not *when* IT pros should begin managing IPv6, but rather what can be done *today* to manage IPv6.

Origins of Shadow IPv6

IT pros may ask how, if they haven't yet transitioned from IPv4, do shadow IPv6 networks exist in their organizations? The reality is that many network devices enable IPv6 by default—think expansion, BYOD or system lifecycle replacement.

So, even though IT may not have formally made the switch to IPv6, it's actually natively enabled on the network—and just like an open TCP can pose security risks, unmanaged IPv6 raises security concerns.

It should be noted that while IPv6 does not inherently make the network less secure; it is neglecting to actively manage IPv6 that can introduce security risks. For example, the existence of IPv6 on the network introduces the need for new processes and controls for comprehensive IP address management, and for those who haven't actually transitioned, these likely have not been implemented.

Without these new processes and controls, there could be a covert route in and out of the network, presenting security vulnerabilities that can go undetected.

Eliminating the Risk by Tackling IPv6 Now

To truly bridge the IPv4-IPv6 gap and avoid security issues associated with shadow IPv6, there are several best practices IT can employ now, before it's too late.

First, IT pros should try to simplify the whole process of IP address management—for both IPv4 and IPv6—in order to eliminate network conflicts and outages, track critical assets, ensure network security and provide reports based on a wide range of parameters, including IP address status.

In terms of processes, IT should identify and document devices that currently support IPv6, map existing IPv4 space and proposed IPv6 space and document devices that need to be added/replaced for IPv6 support.

Finally, to find the shadow IPv6 already lurking on networks, IT should take the following into consideration:

- *Multicast:* IPv6 does not support IPv4 "broadcast" addresses. Rather, it expands the use of multicast addresses and can be used to deliver additional capabilities like service solicitation and address resolution. As a result, well-known multicast addresses may be exploited to reveal unpublished resources like critical core devices or application servers. Once identified, these resources then become the target of more malicious actions. To combat this issue, IT pros should carefully manage and explicitly enable multicast configurations and associated protocols and services as needed.

- *Stateless Address Auto-Configuration (SLAAC):* IPv6 provides a default, automated method for an IPv6 host to obtain an IP address without manual configuration or interaction with a DHCP server. This means it's possible for a device to operate stealthily on a network. To manage this risk IT should disable SLAAC and use DHCPv6. This will provide a single means of maintaining visibility and controlling access to the network.

- *Security Controls:* It's entirely possible that some security controls (e.g., firewalls, filters, NIDS, etc.) either don't work with IPv6 or have not been configured to work with IPv6, which can potentially let IPv6 hosts onto the network undetected and IPv6 traffic go unmonitored. Many studies document how malicious tools can be used to detect IPv6-capable hosts, take control of IPv6 auto-configuration and begin tunneling IPv6 traffic in and out of IPv4 networks undetected. One way to address this risk is to either verify appropriate IPv6 security controls are in place, or aggressively filter or block IPv6 traffic as needed.

- *Vulnerabilities:* Many vendors have supported IPv6 for a number of years, but the process of hardening these implementations is ongoing. As a result, new vulnerabilities will inevitably be discovered and exploited, which can lead to a loss of system confidentiality, integrity and availability. To combat this, it's important for IT to identify at-risk hosts and actively manage security updates.

The fact of the matter is that IPv4 and IPv6 will continue to coexist for the foreseeable future, further compounding the risks of shadow networks.

There will be an ever-growing need to identify and track IPv6 devices; concurrently manage IPv4 and IPv6 address blocks, DHCP and DNS services; monitor IPv4 and IPv6 resources and tasks and reduce administrative burden when IP-connected devices continue to proliferate.

To sustain future growth, the most effective way to manage the shift is to allow networks to support both IPv4 and IPv6 simultaneously—the end result will take tremendous burden off of network administrators by providing centralized visibility and management while having a positive effect on network uptime and security.

IT should equip themselves with the knowledge, skills and tools needed to bridge the gap today, not only to prepare for the imminent transition to IPv6 in the future, but to mitigate the security risks associated with shadow IPv6 today.

About the Author

Chris LaPoint is the vice president of product management at SolarWinds, an IT management software provider based in Austin, Texas. Chris leads the company's fanatical devotion to understanding customer needs and delivering user-centric products that solve real problems. He has spent the past decade building IT management software, first as a software engineer, then as a technical evangelist and product manager. Prior to SolarWinds, Chris' held positions with Sun, UnboundID, NetIQ, Pentasafe and Tivoli.

THE LARGEST CYBER CONFERENCE IN ISRAEL!

CYBERTECH2015
THE EVENT FOR THE CYBER INDUSTRY

ISRAELDEFENSE | PRIME MINISTER'S OFFICE NATIONAL CYBER BUREAU | State of Israel Ministry of Foreign Affairs | Ministry of Economy | Ben-Gurion University of the Negev

THE INTERNATIONAL CONFERENCE & EXHIBITION FOR CYBER SOLUTIONS

CYBERTECH 2015

24-25.3.2015 | TEL AVIV, ISRAEL

Register Now!

Through the conference website or by telephone: +972-74-7031211

WITNESS AND EXHIBIT THE LEADING CYBER INNOVATIONS FROM AROUND THE WORLD!

ORGANIZED BY: ISRAELDEFENSE

FOR MORE INFORMATION AND REGISTRATION:

E: cyber@israeldefense.co.il | www.cybertechisrael.com | T: +972-74-7031211

A Smart Configuration of Your Computer… How Good is That as a Prevention from a Hacking?

Milica Djekic

Computer breaches, hacker's attacks and cyber incidents are becoming a part of our reality. Once a malicious actor is inside your system, it's quite difficult to protect your cyber asset from being exploited. But, are there any preventive measures that could support you in your intent to stay cyber safe? It appears one of the best ways to prevent your IT system from a hacker's attack is to configure your computer smartly. In this brief review, we plan to deal with some tips on how to configure your cyber system and stay away from the bad guys.

What Are the Issues at the Moment?

As it is known, there are many issues with the cyber threats of today worldwide. It's not that rare of a case that malicious actors break into someone's system and cause a significant amount of damage. Using a modern hacking management tool such as, for instance, an open-source Armitage or similar software, hackers can see what is going on in someone's computer while that person or organization is online.

Here, we could use the old joke that says the best way to stay away from the cyber threat is not to buy a computer at all or even if you decide to take that risk, you should never use your internet connection. Well, in a modern world where everything is vitally depended on computers, it's quite hard to imagine any of these two scenarios to find their applications in the practice.

So, we have the bad guys on the one side with their pretty cheap hacking management solutions, but still good enough to cause a headache to all of us and we have the valuable information of the other side which should get protected. What we suggest here is to try to configure your cyber assets smartly and, in that sense, prevent your IT system from being exploited.

In this article, we plan to identify the key points in your cyber infrastructure that could be vulnerable in cyber terms and also propose some bright solution to each of those issues.

How to Protect Your E-mail Account?

As one of the most concerning points within your IT asset, we would identify your e-mail account. It appears it's easier than ever to get access to someone's mail. With that access data, you can easily log into someone's account or even stealing the mails from such a person or institution.

In practice, it's quite simple to do so using one of the public e-mail services. Many of them have the option that will allow you to re-direct copies of the e-mails from someone's account to yours. You can imagine what would happen if some of the government's departments would be exposed to this sort of cyber espionage.

For these reasons, we suggest that everyone should use security features for a cloud-based e-mail clients or security plug-ins for a computer-based e-mail solutions. It's quite easy and convenient to find the most suitable plug in that fits your e-mail client and to use it in order to increase security to

your system. In other words, if you smartly configurate your e-mail account, you would remain cyber safe from the threat that intends to do harm within your e-mail correspondence.

Also, many public e-mail services offer an opportunity to set up your security option and, for instance, choose your own computer or laptop to be the trusted one or you can even select that the one how steals your mails sees them as unreadable. You would agree it's quite good and convenient way to protect your assets.

How to Deny a Remote Access to Your Computer?

As we said, the best way to stay away for the bad guys is to deny their remote access to your computer. In Figure 1, we illustrate a significance of the smart configuration of your computer as well as a denied access to malicious actors in sense of the safe cyber system.

Figure 1. How to get cyber safe?

As explained before, the biggest issue with the modern hacking tools is that the bad guys can take a remote control over your computer and they can see on their screen what you do on yours. When they see you are struggling, they will get more motivated to attack.

Luckily, many commercial operating systems of nowadays offer an opportunity to set up your options for a remote access. You do not need to be an expert, it's enough to be an advanced system's user to choose a smart configuration for your computer that could prevent you from cyber incidents and keep the bad guys away from you private or business information.

Here, we strongly recommend to try to play with your remote access options on your, say, Windows, Mac or Linux machine and attempt to figure out which configuration is the most suitable in terms of denying an access to malicious actors.

Also, it may appear as quite convenient if some organizations or businesses would invoke such a security procedure and use it on regular basis, because it could be a pretty good way for them to

get protected from hacker's incidents. That's only an idea how this advice could be applied in the practice.

Final Comments

At the end, as we always say, a security is the process of maintaining an acceptable level of the risk. In a cyber world, we deal with a cyber risk, so we could use a similar definition for a cyber security. In this article, we only try to make some suggestions and give some advise in terms how to remain cyber safe, but in practice if you really want to remain secure, you have to put a lot of effort every single day in order to maintain your condition. The idea to select a smart configuration to your computer could be the good one, but there are still many suggestions and advice that should be used in everyday's life and researched better in the future.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications. She writes for Australian and American security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

The Power of UDADS in HIPAA Compliance

As cyber threats proliferate across the globe in the past few years, HIPAA requirements have increasingly become more stringent forcing companies that deal with private healthcare information to take swift, compliant action. The goal for a healthcare organization's business, audit, compliance, risk, and security disciplines is to not only protect the information of both customers and employees in their organization, but to also make the protection of such information a fundamental core business principle that all companies that conduct business with the healthcare organization are obliged to follow in order to prevent future data breaches and medical information thefts.

HIPAA compliance is no longer just an audit, compliance, and risk discussion; this is becoming an overall business discussion. Following the 2014 data breaches of companies like Sony, JP Morgan Chase, Goodwill Industries, and The Home Depot to name a few, any leniency that the Health & Human Services Department once had for companies violating HIPAA requirements will likely vanish. The tremendous publicity that data / security breaches outside of the HIPAA discipline have generated will create more pressure on the Health and Human Service's Office for Civil Rights (OCR) to enforce HIPAA breaches. Interestingly enough, HIPAA has a plan to launch its own audit program in 2015 which will audit all covered entities and their respective business associates.

With these upcoming audits and requirements, it is safe to say that the Health & Human Services Department is looking to crack down on negligent, reckless healthcare data protection and cyber security practices around HIPAA data. I expect updated HIPAA requirements and audit information to be released in the upcoming months that will result in unplanned data protection and cybersecurity initiatives becoming a boardroom topic to ensure their organization is compliant in 2015.

Over the years, I have developed a number of security and data protection programs for healthcare, financial services, pharmaceutical, manufacturing, retail, and information technology industries. What I have learned is that there are a few simple recommendations when developing a HIPAA compliant program that fundamentally will provide the building blocks for successful HIPAA audits and I call that UDADS. User; D – Data; A – Audit; D – Data ; S – Secure). Please note that data is referenced twice – you will see why below.

User (employee, contractor, vendor, and third-party provider) authentication/authorization:

- Each system user should have a unique identifier (i.e. unique user name);
- Automatic Logoff: User's session has to be terminated after a fixed time of inactivity; *- this can have a significant impact to business operations; therefore, make sure business leaders / champions understand "why this is important to their business, their customers, their brand"*
- Backend part of the system must verify User's permissions to execute an appropriate operation and must allow it only for authorized Users – *no "generic" accounts e.g. user 1, admin 1)*
- Web Application has to be protected from cross-site request forgery (CSRF) attacks *– this attack vector is still one of the simplest to protect against but often exploited by cyber criminals*

Data validation:

- Data validation has to be performed on both client and server sides.
- Protection from SQL Injection should be adjusted. Validation logic can be placed on different levels of application. – *this attack vector is still one of the simplest to protect against but often exploited by cyber criminals*
- Protection from Cross-site Scripting (XSS) should be arranged. – *this attack vector is still one of the simplest to protect against but often exploited by cyber criminals*

Audit Log:

- Each operation/action with protected health information (PHI) record(s) like Create/Update/View/Print/Download must be stored in Audit Log. The information that has to be logged includes:
  - Who performed an operation/action?
  - When was an operation/action performed?
  - What operation/action was performed?
  - Which protected health information (PHI) record(s) was/were impacted?
  - How protected health information (PHI) record(s) was/were changed (as a result of the Update operation)?
  - Patient's identity.
- Each login action (successful and unsuccessful) in the system has to be logged in Audit Log.

Data storage:

- System should not log any protected health information (PHI) data into unprotected log storage;
- All protected health information (PHI) data that is stored locally (local storage, cookies, etc.) must be encrypted;
- All passwords should be stored as hashed values;
- Data storage(s) must be backed up on a daily basis and can be recovered in case of an emergency or accidental deletion. Regular backup procedure has to be established.
  If a system sends information elsewhere (for example, via email), then these messages should also be backed up or archived. Make sure that the backups are robust, available, and accessible only to authorized people.
- Access to data storage(s) should only be provided to authorized personnel:
  - All connection strings in Web/App configuration files or system registry have to be encrypted;
  - All backups have to be stored in encrypted state.

- Data storage should not be located outside of the USA;
- System should not allow physical removal of the protected health information (PHI) records. Just mark these records as inactive instead of deletion

Secure data transmission:

- Client-server communication should be performed via secured channel (SSL/HTTPS);
- Client should not pass any protected health information (PHI) data in URL parameters when sending a request to the server;
- All data transmission outside of the system should be done via secure protocol (HTTPS, Direct Protocol, etc.).

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.

INTERPOL WORLD 2015

14 - 16 APRIL 2015

Sands Expo & Convention Centre, Singapore

PLAN YOUR VISIT NOW

CYBERSECURITY

BORDER MANAGEMENT

SAFE CITIES

SUPPLY CHAIN SECURITY

YOUR PARTNERSHIP PLATFORM

INTERPOL *World* Public-Private Partnership

- Game-Changing catalyst of innovation to address global security challenges

YOUR SOURCING & BUSINESS PLATFORM

INTERPOL *World* Expo

- 250 exhibitors from over 25 countries
- Be the first to view new and innovative technologies

YOUR KNOWLEDGE & NETWORKING PLATFORM

INTERPOL *World* Congress

- Launchpad of co-created innovative solutions with leading private-sector security solutions providers

EARLY BIRD ENDS 27 FEB 2015
(LIMITED SEATS ONLY!)

YOUR BUSINESS AND NETWORKING ENGINE

Register online now at www.interpol-world.com

Event Owner: INTERPOL

Supported By: Ministry of Home Affairs; iesingapore – Driving Singapore's External Economy; Singapore Exhibition & Convention Bureau

Supporting Knowledge Partner: Frost & Sullivan

Held In: YourSingapore

Managed By: mp

What NOT to do When You've Been Attacked

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

Sometimes knowing what NOT to do in the event of an emergency can be just as important as what you SHOULD do. For example, don't throw water on a grease fire; don't run if you encounter a bear in the woods; and don't leave the scene of a car accident. There are similar rules of thumb when dealing with the aftermath of a cyberattack.

In a previous article I talked about the five things to do to effectively and efficiently handle an attack and minimize the damage done. Once a breach happens the consequences can be devastating. But acting too hastily can lead to missteps that may expose the organization to additional attacks, hamper the investigation, or slow response.

Here are three tips on actions to avoid:

1) **Don't tip your hand needlessly.** You may decide to contain the attack but be careful how you respond. Actions such as hacking back or submitting the malware to a reporting site will inform the adversary they've been discovered.

   The same is true if the team uses the compromised network to coordinate incident response efforts, rather than establish out-of-band communications. Hackers will deploy another technique while the team is distracted and busy dealing with the first attack.

2) **Don't start investigating without a plan.** An overzealous response can compound the damage.

   For example, utilizing an external tool to attempt to find the threat can taint the data required to perform proper timeline analysis and inspect other important information such as prefetch data (data that is preloaded to speed the boot process and shorten application startup time). Prefetch data can provide valuable forensics artifacts that might help answer the "what", "where" and "when" of an attack.

3) **Don't keep it to yourself.** Inform management and the right people using the incident notification call list and call tree. Collaboration can help to more effectively deal with the situation.

   For organizations that choose to hire professional services to help, make sure knowledge transfer is part of the process to help keep costs in check.

When an attack happens seconds count. The 2014 Verizon Data Breach Investigation Report found that in 75 percent of cases the breach wasn't discovered for weeks, months, or even years. But it typically only took hours or minutes for the attacker to accomplish the mission.

You want to act swiftly, but you don't want to make matters worse with uninformed actions.

To learn what you SHOULD do in the event of an attack, take a look at our eGuide, ""Five Things To Do After You've Been Hacked," which provides you with a plan of action to improve your response and mitigate the impact of attacks now and in the future.

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

IBM: Proven to withstand the tests of time.

Companies all over the world have found ways of integrating IBM systems in a rapidly changing technological environment. No company however, has been more adept at adjusting to change than IBM itself.

After all, IBM has always been a major innovator. When the S/360 was born 50 years ago, it was unlike anything that had come before. For the first time computers were affordable, at least for big businesses. The S/360 was technologically brilliant, introducing IBM's Solid Logic Technology, for instance, which made the machine much smaller and faster than its competition.

According to Computerworld

http://www.computerworld.com/article/2488997/mainframe/mainframe-turns-50--ibm-system-360-launch-was-dawn-of-enterprise-it.html, one of the most revolutionary aspects of the S/360 with the idea that the same architecture could be shared by less expensive machines and the high-end models. This gave the entire line upwards and downwards compatibility, and so successfully that programs written for the original S/360 will still run on contemporary machines. The compatibility helped IBM sell as many computers as possible, which it needed to do—the S/360 was initially projected to cost $675 million, but its final cost was $5 billion.

It's certainly been worth it. IBM machines supply some unique attributes, and they still get plenty of use. The demand for MIPs, or millions of instructions per second, is growing all the time—per Compuware, at a rate of 41% per year—and IBM machines are still the go-to technology if you need MIPs. Will we ever *not* need IBM? According to a fascinating history of the company in *The Register,* CIOs are predicting at least another decade of IBM dependency. http://www.theregister.co.uk/2014/04/07/ibm_s_360_50_anniversary/?page=1

When *The Register* asked to speak to a typical IBM customer, they were surprised to be referred to a new cloud startup, L3C, now owner of a BC12. L3C thinks it can put enough virtual machines on the server to make it an economical choice. Linux is another newer technology that's very at home on IBM machines; in fact, it's an IBM smash hit. Linux is available on System Z, and it's the language that 60% of System Z customers want. The IBM–with–Linux setup is growing at a rate of about 30% per year.

And maybe more companies should be taking IBM machines to new heights. Computer Weekly suggests that more tier 1 service providers should be looking to IBM, and they have the numbers to prove it.

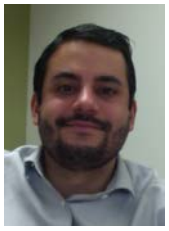
"A 2012 study from WinterGreen Research demonstrated the savings of an IBM zEnterprise 114 mainframe over a VMware setup using HP ProLiant DL685. WinterGreen Research calculated that a suite of Linux web services applications running on 80 HP blade servers with VMware would cost $127,225 a year, while the same application configuration on the zEnterprise 114 would cost $67,787. The zEnterprise 114 (or z196) server is cost-efficient because it uses less power and fewer software licenses, the study said." http://www.computerweekly.com/feature/Can-the-mainframe-remain-relevant-the-cloud-and-mobile-era

IBM is eager to be seen as a suitable cloud platform, and it's been adjusting its prices accordingly. It announced the IBM Enterprise Cloud System for about $75,000 last summer. This is very similar to the machine that cost $1 million back in 2003. The Enterprise Cloud System includes a Linux server and the so-called IBM Cloud Management Suite, which includes software for the configuration and deployment of virtual machines.

The recent zEnterprise EC12 is typical of the kinds of machines IBM turns out today. Its development represents an investment of more than a billion dollars. It's incredibly fast—more than 78,000 million instructions per second. It has special cryptographic abilities which permit it to be ultra secure and to process signatures and passports. It monitors itself and recognizes any unusual deviations in behavior. It can ramp up to provide maximum availability during periods of heavy use. It has special processing to support concurrent transactions. It has the world's fastest chip. It's cloud ready.

It all makes you wonder—maybe IBM won't just be around in 10 years, maybe it will be more dominant than ever. One thing's for certain—the technology developed by IBM is going to remain a force to be reckoned with for many, many years to come, and how IBM technology is to be integrated with the rest of the technological landscape is an issue that won't go away soon (if ever).

About the Author



Mike Miranda is a writer and pr person for Rocket Software.

International Relations Theory and Cyber Security

By: Artin Amirian

National Cyber Security is the latest addition to International relations and strategic warfare studies. War strategists throughout documented war history have used contemporary technologies to improve their offense and defense capabilities against their adversaries, but technology has always been an ancillary provision to complement the classical weapons and "boots on the ground" forces; Catapults were first utilized to break barriers so the armies and soldiers could walk behind tall walls of an empire and during WWII communication engineers and code breakers used technology to collect intelligence against their enemies, but technology has a different role in the domain of warfare today. Information technology has independently become both an offensive and defensive weapon.

Right after the Second World War, international relations (IR) theorists used Nuclear Weapon proliferation as a benchmark theorizing about the behavior of the international system, but the new kid on the block (cyber weapon) has introduced new sets of dynamics and parameters that will change the game dramatically. To understand the complex world of international relations it is imperative to consider the political ramifications and theoretical perspectives that will define how states will see cyber capability as a weapon of choice for their future conflicts. One may ask why we need to understand these political theories and International Relations studies. Aren't we engineers and IT professionals that our work is to secure networks? I agree, we are IT geeks but the problem chose to knock on our door.

Cyber security is a synergy between the government and the private sector; no sovereign state should claim that they can secure their cyber space only utilizing government resource, so yes, as IT professional we are part of the problem and as a matter of fact we are at the core. It is our responsibility to understand the effect of our work, we each contribute to the security of this vast interconnected network of LANs, WANs and MANs and the aggregation of our work may develop a threat to national security, if we are not aware of the technical and policy implication of our work.

IT professionals are usually associated with technocratic qualities to problem solving but this seems to be a totally different game we are getting into so dear colleagues the onus is on us to understand the bigger picture and understand the potential risks that our systems may impose on national security. Let's understand cyber warfare capability and its effect on national security from two dominant theories of IR, Realism and Idealism.

Realism

Realism claims that the offensive Cyber warfare capability of weaker states against the hegemon in an asymmetric balance of power provides a strong strategic advantage for the weaker (rising hegemon) state. Realism is a state centric international relations theory that emphasizes the role of security in international politics. Considering the notion that states are constantly looking for opportunities to maximize relative power, the realist context of zero-sum gain and "security-

dilemma" forces the international systems to improve their offensive capability in order to improve their odds of survival and defend their national interests.

For a weaker state that is constantly in the act of balancing power and increasing its power position in the anarchic system of international relations against the hegemon, these strategic and guerilla war capabilities are consequential and arguably the only challenging method against a strong militarized rival.

One may argue that there is still a significant "digital gap" between haves (having strong technological and cyber capabilities) and have-nots, attributing a stronger cyber warfare capability to states with stronger military and technological advantage. However the difference between developing a strong cyber warfare capability and nuclear capability is substantial. It takes less economic, human and geo-political resources to develop cyber-attack capability than nuclear capability.

Realism defines military capability as the currency defining power in the anarchic international system. Also one of the fundamental assumptions of realism lies in the essential role of states as the main and the only relevant actors in the international system.

Going back to the fundamentals of realism and trying to fit the cyber war capability and its strategic relevance in today's world, it is apparent that all basic assumptions of realist paradigm -which can be defined as, international system is an anarchic system, primary decision makers are rational acting states with goal of satisfying the interest of survival by changing the balance of power in their favor- are staying unchanged by the introduction of cyber warfare capability.[i] Does cyber warfare capability undermine any of these assumptions?

Cyber warfare including both defensive and offensive capabilities not only does not undermine these assumptions rather it fits well with the theory. First, there is no over-arching organization or world system that regulates cyber space (cyber space is anarchic in nature). Second the major cyber assaults and attack resulting in colossal national security threats will require sophisticated software and hardware capabilities that can arguable be provided and supported by nation-states.

Third cyber warfare follows the rationality argument of the realist paradigm, retaliation in cyber warfare can be both in the form of cyber attack and conventional attacks thus defining the cyber warfare capability in the same level as Kinetic (conventional) war, states should rationally act upon their decision to utilize cyber attacks since cyber attacks just like conventional attacks can constitute a risk to national security.[ii] "Rationality" of the actors inherently assumes the "cost-benefit" analysis as the basic form of decision making in the anarchic international system.

The cost of entry into cyber war in contrast to conventional war is incredibly low. In a cyber attack the benefit of attacking an adversary far outweighs the dangers and risks of conventional war. This has also made cyber war a viable military capability for state-actors.

Another prevailing argument supporting the importance of cyber warfare strategic capability against stronger states is embedded in the fact that hegemons and militarily developed states tend to be more reliant on cyber platform thus providing a strong advantage for challengers and rising

hegemons to use that weak point and attack their cyber and network infrastructure, resulting in destruction and compromising the integrity of their military information.

Such strategic advantage can place cyber offense capability at the top of the military agenda for weaker states. Also the stronger states should consider their vulnerable information infrastructure as a major national security threat trying to develop complex defensive systems to fight against such breaches of security.

If a state chooses to invest in developing a strong team of offensive cyber warriors or invest in developing technologically advanced systems to have offensive capability, this will consequently undermine the cyber security of others. The asymmetric and surprising nature of cyber attacks makes it harder for the defender to detect and deter attacks. Another important implication of the security dilemma lies in the defensive aspect of cyber warfare. In a kinetic (conventional) war the effect of a bomb is equal, independent of the "development status" of the state it is dropped on. However cyber capability by nature provides an asymmetric balance of vulnerability in the defensive perspective. Stronger states are more vulnerable in an anarchic system.

Another distinguishing characteristic that cyber warfare presents in the context of strategic studies and security dilemma is the fact that it is harder to qualify and quantify the cyber capabilities of your adversaries, unlike the conventional war that you can verify their military basis and their physical assets (i.e. bombs, warheads, tanks and artillery). This provides a major strategic advantage for weaker states because such covert development of cyber capability does not raise flag for their stronger adversaries to build up militarily against them.

Considering all these theoretical perspectives in the context of "Realism" it is clear that cyber war capability provides a substantial strategic advantage to the weaker state in an anarchic world of rational actors trying to shift the balance of power in their favor. Realism is a sound framework addressing the viability of developing offensive capability for state actors, especially weaker states against their adversaries.

Idealism

Idealism argues that the effectiveness of a rising hegemon's strategic warfare capability is not strongly affected by cyber warfare. Idealism relies on globalization and the effect of technology on global system of economic and political interaction. Idealism also claims that cyber warfare by nature does not impose major security threats on the state, since without the effect of kinetic warfare capability the result cannot be devastating enough to be considered a serious national threat.

The information revolution, the creation of cyberspace, and high technology's impact on globalization are often cited in support of idealist arguments that emphasize the role of technologies, such as the Internet, in enabling democratic movements, globalizing financial markets, and sustaining international organizations. On the other side of the spectrum from realism, idealism argues that inherent borderless nature of the internet and the fact that it has been the pillar of globalization qualifies it to be a medium that has created cooperation in the international system.

The most important contributions of idealism theory to the discipline of IR can be summarized as: first, the importance of the plurality of international actors (international system is a collaborative framework for states), second, the importance of domestic political factors in determining the international behavior of states (internal affairs and domestic policies define the international relations, not the balance of power argument), Third, the role of international institutions in establishing rules of behavior (or regimes) for state actors (UN as the main organization and others such as WTO, and other NGOs) and fourth, expanding the agenda of international studies (particularly in the subfield of international political economy) by focusing on a broader set of issue areas than mere survival and balance of power argument.

Idealism agrees that states are important actors in the international system however it does not see states (like Realism) as the only actors. Non-state actors such as NGOs, Terrorist organizations, transnational organizations and interest groups also tend to have major role in the international system. Idealism unlike Realism argues that the positive outcomes of interdependence and interconnectedness are more important and definitive factors in international system rather than the increasing vulnerability and insecurity inherent in realist argument.

With recent development in cyber-warfare capability one may pose the question to liberal scholars about the effect of cyber warfare capability on the international security. “Many nations have aggressive computer-warfare programs, and that with a few keystrokes, an anonymous source anywhere in the world might break into and disrupt the (private) power grids of major cities.”[iii] Soft power is becoming more apparent and influential in the technologically savvy world. Liberal scholars also use the inherent collaborative and open source nature of internet to create a synergy between their theory and cyber space.

The expanding partnership between the public and private sectors to provide cyber security and services attests to the fact that states are not the only actors involved in national security, for example many large defense organizations such as Department of Homeland Security use private contractors to develop military cyber security platforms for national security purposes, such collaborations are not identified in the realist theory.

“To realists, globalization reflects the hegemonic influence of major powers in international politics. Realists tend to see proximity creating vulnerability, which leads to conflict.”[iv] Cyber warfare capability has only been possible due to such cyber imperialistic ambitions. Concepts such as participation in global economic system have mandated many states to internalize technological and cyber frameworks in their national security system and create a major source of vulnerability for their national security.

Idealism does not assume that states are rational actors, and does not discount the notion of rogue actors in the international system. Also idealist theory claims that states are not unitary actors, they tend to respond to many variables such as institutions, groups and identifiers in their sovereign territory. For idealist theory domestic policies have major significance on international relations. It is true that cyber space has created an open global system of communication, but at the same time this openness is the inherent risk that has imposed on states that do not recognize the cyber-attacks as serious threats to their national security.

If you cannot identify the cyber-attacker, you cannot impose penalties. This provides a strong strategic advantage to cyber warfare capability as a weapon. Idealist theory assumes international system as a complex matrix of intentions, besides power and military might there are many domestic, foreign policy and economic issues that define the complex relationship of states. Inserting nuclear proliferation in this context provides a strong contrast in approaching the global system from idealist view.[v]

Both Realism and Idealism provide us with frameworks to understand the National Cyber Security in the context of IR theories, as this article may sound too "Policy-like" and "Social Science-ish" it is important for us, IT/security professionals, to understand the effect of our work on developing the national security doctrine.

About the Author

Artin Amirian is an IT infrastructure engineer with extensive education in Computer Science, Economics and International Political Economy. His graduate research has focused on cyber security policies, globalization of information technology and the implications of CNOs on national security. He currently directs the engineering department of TeraBand Technologies, a California Based IT design/integration firm and continues his research on the effect of information technology on national security.

[1] John J. Mearsheimer. *The tragedy of Great power Politics.* New York, NY: W.W. Norton & Company, 2003

[1] John J. Mearsheimer. *The tragedy of Great power Politics.* New York, NY: W.W. Norton & Company, 2003

[1] Nye, J.S, Jr. (2003) *Understanding International Conflicts: An Introduction to Theory and History*, 4th edn, New York: Pearson and Addison Wesley

[1] Sean Kay, "Globalization, power and Security," *Security Dialogue*, vol. 35, no. 1 (March, 2004)

[1] Michael W. Doyle, "Liberalism and World Politics, "*The American Political Science Review* vol. 80, no. 4 (December, 1986)

Featuring the NEW
Cyber Threat Intelligence Zone

REGISTER FOR FREE TODAY

COUNTER TERROR EXPO

21-22 APRIL 2015 | OLYMPIA LONDON

WORLD – INTERNATIONAL SECURITY FOR AN EVOLVING WORLD – INTERN

The event that will bring together information security professionals to mitigate cyber threats and terrorism

- **See** the latest products, services and technology to protect governments, business and the national infrastructure from cyber threats
- **Explore** the latest thinking, case studies and technology in the NEW Cyber Threat Intelligence Zone
- **Learn** how to ensure your organisation is as best prepared as possible to deal with cyber terrorism
- **Network** and share best practice with the international cyber security community

Save £50 by registering for your free exhibition pass at

WWW.COUNTERTERROREXPO.COM/CDM02

Your unique registration code is CDM02

Co-located with

Supported by

Supporting associations

Follow us on

Organised by

Is digital privacy an illusion?

I think the first thing to establish here, is privacy from whom.

Realistically as consumers, we don't have much privacy from third party marketers. For example companies are constantly sending us targeted ads and know our locations.

When it comes to privacy from the government, we certainly don't have it. The government now grabs large amounts of information on everyone in order to find the one person who is guilty. In the past, this was illegal in U.S., but under the FISA warrants this is now allowed, and the previous concept that there must be a probable cause for the government to issue warrants is falling away. Now, the government is doing massive surveillance. The use of tools such as the stingray, which is used by policemen to capture all cellphone signals in the area, is an example of that.

How clear of a picture of someone's life can organizations build with the data available?

It's difficult to find information that isn't known by a company. Today, your phone tracks your location, everything you buy is tracked by the vendor, all your documentation is tracked by government, so maybe the question is really in reverse. Can you name a piece of information that isn't known?

And that's a trick question, because somewhere some company and some government know it. What's stopping companies and people from using these bits of information is the amount of work that it takes to gather all of it information and make it meaningful. In the past the amount of effort was so large that it was impractical. What 's happening now, is that effort is coming down, down and down and therefore becoming practical to do so.

Do consumers have more to hide than they think?

The key here is to ask whom do you want to protect what from. That's the question consumers have to ask themselves today. Do I want to protect my medical information from anyone but my provider? Consumers have to answer that question before moving on. This is because security and privacy today is deciding who gets what, and that comes down to controlling your information.

Right now, we live in a world where the information is controlled by vendors and not the consumers. Things are starting to change in order to address that, and something like Private.me hands back this control to the consumers so that they can decide who views their personal information. So for example with Private.me, users can search the Internet without being tracked whatsoever, and can use a control panel to decide which vendor views their personal information and for how long.

How can the government strike the right balance between privacy and fighting against terrorism?

We choose the balance as citizens, and in many ways we get the final say.

The problem is that digital privacy is such a complex issue that people don't really understand what's going on. This makes it difficult to push or move the government to where we, as a society want them to go because we don't understand the issue.

Digital privacy is going to be very much like global warming ten years ago. It's difficult to get people educated enough to make a decision on the topic. Until we do, it's in the government's interest to push boundaries to their benefits. And the only way to fix a broken system is through education so citizens can make the appropriate decisions.

What consumers can do to increase their digital privacy?

Consumers can do a couple of things. When it comes to social media, consumers need to assume that everything is public, and need to decide whether to engage in it or not.

When it comes to giving information to vendors, consumers don't have much a choice. As consumers we must realize that nothing is free. When using services such as Gmail, we are paying with our information. The idea is personal information in exchange for services. Until we as a society understand that, we cannot start making the appropriate changes.

What is Private.me? What are some key features and why should consumers use it to protect their online privacy?

Private.me is a company that's addressing these issues of privacy and vendors controlling consumers' information. The company that enables Internet-goers to search online without being tracked whatsoever. Through its patent-pending solution, the company encrypts, slices and distributes users' information so that no single entity can access it at the same time. In addition, it has a control panel that enables consumers to decide which third parties have access to their information and for how long.

Essentially, the company is trying to give consumers control over their information and change the paradigm so that the general public has the power, not vendors.

About the Author

Robert Neivert is the COO of Private.me, a company that enables Internet-goers to search online without any risk of being tracked whatsoever through a patent-pending process that encrypts individual's data and distributes them to non-profit distribution centers.

He has over 15 years of experience with technology and consumer relations, and is able to discuss a wide range of topics.

The UK Energy Cyber Security Executive Forum

A one-day conference

London, 5th February, 2015

20% Discount for CDM subscribers

An exceptionally strong speaker panel includes:

- **Ciaran Martin,** Director General for Government and Industry Cyber Security, GCHQ
- **Graham Wright,** Group CISO and Digital Risk Officer, National Grid
- **Stephanie Daman,** CEO, Cyber Security Challenge UK
- **Dr Gal Luft,** Senior Advisor, The United States Energy Security Council & Chairman, Nation-E
- **Raj Roy,** Legal Director, British Gas
- **Iowa Carels,** Senior Cyber Security Advisor, The National Cyber Security Centre, The Dutch Ministry of Security and Justice

…. and many others

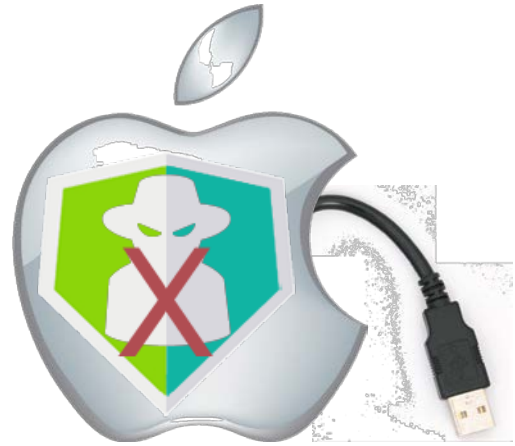
This conference will:

- *Provide insights into the latest cyber security developments in the UK, Europe and the US*
- *Offer C-level executives guidance to minimise the risks, avoid cyber security breaches through proper adherence to standards, develop resilience, protect and strengthen your business in the UK and globally*
- *Supported by Cyber Security Challenge UK, IISP, ISSA, The Journal of Energy Security, The Energy and Cyber Security Center, this strategic and practice-driven summit will give you an excellent opportunity to network with the best of the energy cyber security sector and learn how to actively engage with the cyber security issues at the board level.*

Demand for attendance at the event is likely to be high
Visit www.cityandfinancialconferences.com/CyberEnergy2015 to book
Alternatively email bookings@cityandfinancial.com or call +44 (0)1483 479331
Use code CYSENCDM to obtain discount

Mobile Device Security: Don't Be Naïve

I woke up this morning at my normal 4:30AM. This getting old stuff really whacks your sleep! Turned on the news and the first two stories were on yet another set of cyber security breaches. In fact, there is not a single day that goes by that you don't hear about the latest cyber security breach or credit card hack or personal data theft or even identity theft. This week, a story broke where Sony Pictures had their Enterprise system hacked and unreleased films stolen and placed on the internet for free downloads. Last week, the US Post Office Enterprise got hacked and more than 750k USPS employees' personal information stolen.



WireLurker Malware

But, it isn't just the Enterprise being attacked. Ask Apple. In the past 3 weeks, 2 very nasty attacks were directed at the Apple mobile operating system, iOS. The first is called the "Masque Attack" which poses as a very popular game app and users unknowingly install it. The Masque Attack then steals your banking and credit card transaction information. The other is named "WireLurker", which attacks your Apple mobile device while charging from a USB port. It is an extremely sophisticated program that also steals personal information such as the device serial number, iTunes information, and phone number and sends it to another server.

It struck me that there are just some things that a lot of people just haven't quite grasped yet. The cyber security criminals are very organized. And, there is a distinct shift in their targeting. With the move to more and more mobile device dependency, the criminals are targeting mobile devices more than our desktop and laptop computers. Yes, our mobile devices have become the primary target for cyber criminals.

And the consequences are dire. Think of all the stuff you have on your mobile device. Now think about this. Think about a company of 10 or 20 or 30 thousand criminals. They have the money, the resources, and the expertise. They attack indiscriminately, looking for opportunities, making opportunities, and they no longer have to break into your back door or your vault. They can attack thousands, hundreds of thousands, even millions of potential victims with a keystroke. No one is immune. No operating system is completely secure.

I'm no chicken little. But, honestly, the volume and severity of attacks has me on high alert, especially when it comes to my mobile devices. I have a bunch of them, all Apple. You need to be aware of the ever-present and very REAL threat. You also need to exercise common sense and be smart about protecting yourself from these malicious criminals and their ever-increasing, sophisticated, clever attacks meant to do harm to anyone and everyone. The bad guys don't discriminate.

First, recognize that mobile devices are the new primary target. Be alert. Be cautious. If you receive an email with a link in it that you don't recognize, don't click on it. Doesn't matter if it is your laptop or your iPhone. Seriously, don't do it.

Second, keep your virus protection up-to-date on your computers even though it may be annoying to purchase annual licenses and we are all a little suspicious of the virus protection vendors. But, in the likelihood that you need to connect to your computer with your mobile devices, you don't want to leave an open door for criminals to infect your devices from your laptop.

Third, recognize that juice-jacking is the number one opportunity for mobile device infections - so, when you plug your phone into any USB port, you are extremely vulnerable to attacks. Read up on the recent WireLurker juice-jacking virus and your knees will rattle a bit. You are especially vulnerable while on travel - when you often have no choice but to charge through a USB port and have no way of knowing what you are plugging into. ChargeDefense's product, the Juice-Jack Defender® is guaranteed to block identity theft code and malware when connected to a USB outlet. It's a $15.95 no-brainer. If you don't have a Juice-Jack Defender® and must connect to an unknown USB port, at least keep your mobile device locked. And for goodness sake, put a password on your device! But, even those precautions are no guarantee that a hacker can't find a way in.

The bottom line is this: Don't be naïve. YOU ARE THE TARGET OF CYBER CRIMINALS. Be smart. Protect yourself. Use common sense precautions. And, remember that it isn't just computers anymore. That wonderful mobile device that you carry around with you everywhere needs the same level of protection and precaution as your laptop computer. Be safe.

About the Author

Stuart McCafferty

Like us on FaceBook and get special discount deals: www.facebook.com/chargedefense

THE CYBER SECURITY SHOW 2015

13-14 April 2015,
etc.venues 155 Bishopsgate, London

CYBER SECURITY SOLUTIONS TO HELP PREVENT, DETECT AND RESPOND TO CYBER CRIME

Confirmed speakers include:

Joanne Martin
Vice President, IT Risk
and CISO, IBM

Brian Brackenborough
CISO
Channel 4

Ed Tucker
Head of Cyber Security
HMRC

John Harris
Group Information Security
Manager, Vodaphone

Visit the website for more information: www.terrapinn.com/cybersecurity15

No, It Was Not Cyber Terrorism

Why the Attack on attack on Sony Pictures Entertainment (SPE) Was Not Terrorism

by Edwin Covert, CISSP, CISM, CRISC

The recent attack on Sony Pictures Entertainment (SPE) has garnered a lot of attention, both in the popular media (Katersky & Newcomb, 2015) and in the cybersecurity press (Krebs, 2014). While there is ample debate about who attacked SPE, much of speculation centers on North Korea. I am not going to dispute any of the evidence either for or against the Hermit Kingdom. My dog in this fight focuses on this: Those who call it cyberterrorism; it was not a cyberterrorist attack.

A (Short) Timeline

The Guardian (Shoard, 2014) website has a good timeline of the events leading up to the attack on SPE. In the early part of the summer of 2014, after Sony released the first trailer for *The Interview*, North Korea began protesting on the international stage about the movie (Shoard, 2014). These protestations continued through the rest of the summer and into early autumn. In November, SPE announced it had been hacked by a group called Guardians of Peace (Shoard, 2014). In December, the FBI announced it had evidence connecting the North Korean government to the attack (Laughland & Rushe, 2014). However, others have suggested that an insider was responsible for the attack (Spargo, 2014). Companies such as Norse (CBS Interactive, 2014) and CloudFlare (Rogers, 2014) both cited technical evidence to back up their claims.

Was It Cyberterrorism?

When people use the word terrorism, instinctively we understand what that word connotes: the 2001 attacks on the Pentagon and the World Trade Center, the transportation bombings in London and Madrid, the Achille Lauro hijacking, or the Black September attack at the Munich Olympics.. Constant use of the word "terrorism" has led to people believing that terrorists using computers are automatically cyberterrorists (Mueller, 2012). This is not the case.

The US Department of State defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience” (US Department of State, 2012). While others have provided variations on this theme, I use Hoffman’s (2006) definition as the standard: a calculated use of violence or the threatened use to force a political change by non-state actors. Simply “being” in cyberspace does not satisfy either definition of terrorism.

"Cyberterrorism is non-state entities using computers or information systems to cause politically motivated damage or destruction to information, computer systems, and/or computer programs that could result in violence or the threat of violence against innocent people.(Conway, 2002). In this vein, Ahmad and Yunos (2012) describe five key criteria an act of cyberterrorism must satisfy. The act must:

Be motivated to change policy and lead to death or injury

Cause fear and/or physical harm through cyber techniques

Be against a critical infrastructure sector such as financial, energy, transportation, and/or government

Target essential services

Not have financial gain as its primary motive

Applying these simple criteria to the SPE attack shows that it is not act of cyberterrorism. The target was SPE, not a political entity. As a commercial organization, SPE is not in the business of setting national policy. While the attackers certainly threatened violence against those theaters that screened the movie (Lang, 2014), most people would not consider cinemas critical infrastructure sectors under current policy (US Department of Homeland Security, 2014), nor are movies essential services. Because the motive is truly indiscernible, the debate surrounding the source of the attack rages on (Laughland & Rushe, 2014; Rogers, 2014; Spargo, 2014),. In totality, we have the attack against SPE meeting only one of Ahmed and Yunos' (2012) benchmarks: fear of physical violence. Though significant, fear alone does not qualify the attack as cyberterrorism.

Then What Was It?

For the sake of argument, let us assume North Korea is responsible for the strike on SPE. Any implication of state-sponsorship of such a cybersecurity incident would constitute an act of war according to some (Shiryaev, 2012). If a country uses its territories or assets in attacks against other states, it would be a violation of the International Court of Justice (Shiryaev, 2012). Shiryaev (2012) further notes that the 1970 Friendly Relations Declaration of the United Nations requires countries not to shape, initiate, support, or contribute to terrorist acts against other nations.

While he does say, "If one country organizes, actively supports, or contributes to the commission of one or more terrorist offences through cyber-space, it can be said to be a state-sponsor of cyberterrorism," (Shiryaev, 2012, p. 151) this was not a terrorist attack per Ahmed and Yunos (2012). Unfortunately, this is all new territory; to date, no country has admitted to conducting a large-scale cyber assault against another nation.

On the other side of the assumption, North Korea had no role in the attack on SPE. In that case, the definition is easier to understand: it is cybercrime. McQuade (2006) defines cybercrime as using a computer (or related electronic instrument) to conduct unlawful activities. Cybercrime is pervasive in the US. A recent survey by cybersecurity software firm McAfee and the Center for Strategic and International Studies (CSIS) asserts cybercrime cost the nation upwards of $100 billion in annual losses and as many as a half-million jobs in 2013 (United Press International, 2013).

If the Guardians of Peace is just another hacker group looking to gain financially from the SPE attack or simply make a name for itself, its activities make it an organization that commits crimes against companies–significant and interesting, but not cyberterrorism.

Why Does This Distinction Matter?

The attack against SPE is a serious issue. It could end up costing the company approximately $100 million according news sources (Richwine, 2014). While financially less impactful than other attacks Sony has endured over the years, it is still substantial. However, a crime is a crime is a crime, right? Should we really care about why it was committed or how we classify it so statisticians can sleep better at night? I believe overusing terms like cyberterrorism is a disservice to the American public. Every time the media calls something cyberterrorism when it is not, the public gets an incorrect idea of what the Internet is and what it is not. We, as professionals, need to challenge this incorrect usage. If we do not, we are guilty of spreading the fear, uncertainty, and doubt (FUD) we lament in others.

Conclusion

The SPE attack was a major event. It was an attempt to censor a company from performing its mission through criminal activity and threats of violence. The appropriate authorities should be investigating the attack and working diligently through the process of attribution and then prosecution (in whatever form that takes: criminal charges or an international response); I have confidence that is occurring. My goal is not to minimize the effects of the attack or put forth a new theory of attribution. Rather, I am interested in making sure we do not mislabel the attack and thus dilute the very real consequences of cyberterrorism.

References

- Ahmad, R., & Yunos, Z. (2012). A Dynamic Cyber Terrorism Framework. *International Journal of Computer Science and Information Security*, 149-158.
- CBS Interactive. (2014, December 23). *Was FBI wrong on North Korea?* Retrieved from CBS News: http://www.cbsnews.com/news/did-the-fbi-get-it-wrong-on-north-korea/
- Conway, M. (2002). What is Cyberterrorism? *Current History*, 436-442.
- Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.
- Katersky, A., & Newcomb, A. (2015, January 7). *Sony hack: FBI director speaks about evidence pointing to North Korea*. Retrieved from ABC News: http://abcnews.go.com/Technology/sony-hack-fbi-director-speaks-evidence-pointing-north/story?id=28061831
- Krebs, B. (2014, December 23). *The case for N. Korea's role in Sony Hack*. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/
- Lang, B. (2014, December 17). *Major U.S. theaters drop 'The Interview' after Sony hacker threats*. Retrieved from Variety: http://variety.com/2014/film/news/major-u-s-theaters-drop-the-interview-after-sony-hacker-threats-1201381861/
- Laughland, O., & Rushe, D. (2014, Decembe 19). *Sony cyber attack linked to North Korean government hackers, FBI says*. Retrieved from The Guardian:

http://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official

- McQuade, S. C. (2006). *Understanding and Managing Cybercrime.* New York, NY: Pearson.
- Mueller, R. (2012, March 01). Prepared Remarks at RSA Cyber Security Conference. San Francisco, CA.
- Richwine, L. (2014, December 9). *Sony's hacking scandal could cost the company $100 million*. Retrieved from Business Insider: http://www.businessinsider.com/sonys-hacking-scandal-could-cost-the-company-100-million-2014-12
- Rogers, M. (2014, December 24). *No, North Korea didn't hack Sony*. Retrieved from Daily Beast: http://www.thedailybeast.com/articles/2014/12/24/no-north-korea-didn-t-hack-sony.html
- Shiryaev, Y. (2012). Cyberterrorism in the Context of Contemporary International Law. *San Diego International Law Journal*, 139-192.
- Shoard, C. (2014, December 18). *Sony hack: the plot to kill The Interview – a timeline so far*. Retrieved from The Guardian: http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline
- Spargo, C. (2014, December 25). *North Korea was NOT behind the Sony hack according to multiple security experts who discredit FBI findings and reveal that a studio insider named 'Lena' may be responsible*. Retrieved from Daily Mail: http://www.dailymail.co.uk/news/article-2887081/North-Korea-NOT-Sony-hack-according-multiple-security-experts-discredit-FBI-findings-reveal-insider-named-Lena-responsible.html
- United Press International. (2013, July 23). *Study puts annual U.S. cybercrime losses at $100 billion*. Retrieved from UPI.com: http://www.upi.com/Science_News/Technology/2013/07/23/Study-puts-annual-US-cybercrime-losses-at-100-billion/UPI-94421374608295/
- US Department of Homeland Security. (2014, June 12). *Critical infrastructure sectors*. Retrieved from DHS.gov: http://www.dhs.gov/critical-infrastructure-sectors
- US Department of State. (2012, May 30). *Country Reports on Terrorism.* Retrieved from US Department of State Bureau of Counterterrorism: http://www.state.gov/j/ct/rls/crt/2012/209990.htm

About The Author

Edwin Covert (CISSP, CISM, CRISC) is a cybersecurity professional with over 20 years of cybersecurity and intelligence experience. He works for a prominent management and technology consulting firm in the Washington, DC metro area. He holds the Certified Information Systems Security Professional (CISSP) designation from (ISC)2. He is also a certified Project Management Professional (PMP). He holds two designations from ISACA: the Certified Information Security Manager (CISM), and the Certified in Risk and Information Systems Controls (CRISC). Additionally, he also has held the GIAC Certified Incident Handler designation from the SANS Institute. He works with both government and commercial organizations and is an author on a diverse array of cybersecurity topics. He is a member of the Order of the Sword & Shield, a national honor society for homeland security, intelligence, emergency management and other protective security disciplines. Ed can be reached on Twitter at @ebcovert3.

CVE-2014-7911: Why the ObjectInputStream Serialization Vulnerability Continues to Wreak Havoc

In November 2014 security researcher, Jann Horn, disclosed the ObjectInputStream Serialization vulnerability, also known as CVE-2014-7911. This vulnerability results in a privilege escalation and is easily exploited, which allows hackers to gain administrator level permissions and access to data in any application. What does this mean? If a device is vulnerable to the ObjectInputStream Serialization vulnerability, attackers can easily acquire higher-level privileges than the app that runs the exploit should. This allows attackers to access any data that is stored within any app on device, therefore putting critical user information at risk.

Although disclosure of this vulnerability coincided with the release of Android 5.0 Lollipop, allowing Google to patch the bug, it continues to wreak havoc. Most recently, this vulnerability made headlines after hackers began using it as a means to root Sony Android devices.

This vulnerability allows an app to bypass restrictions by failing to serialize data, which enables an attacker to run code under system privileges and leaves Android devices exposed. It's important to note that hackers can use this vulnerability to root all Android devices, not just Sony ones.

The Details

This vulnerability made the vector of exploit easier and was only patched in Lollipop (released in late 2014), making every device running anything prior to Android 5.0 vulnerable. This leaves a large population of devices exposed since, according to Google's Android stats, Lollipop only makes up 1.6 percent of the ecosystem . However, the Bluebox research team, Bluebox Labs, found that manufacturers have begun to backport a fix. This means they are taking the fix and applying it to older versions of Android. From this we can infer that manufacturers realized this vulnerability was serious enough to patch, based on the fact that a patch to this vulnerability is appearing before vendors issue Lollipop updates. Additionally, some devices may never receive the Lollipop update so backporting a fix makes even more sense in those cases to ensure the security of those devices.

Despite these efforts, a large number of Android devices remain unpatched and unprotected. This means that on those devices an attacker can still:

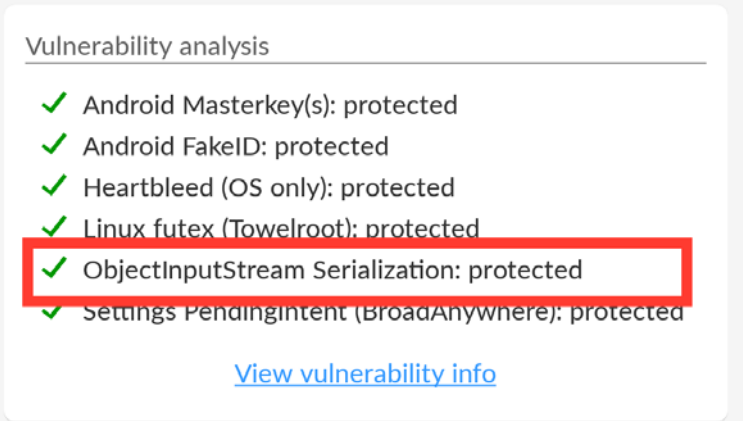
- Gain full control of your Android device
- Access your personal or sensitive corporate information without you knowing
- Install malicious software
- Bypass important security restrictions you or an administrator places on the device

Are your Android devices vulnerable?

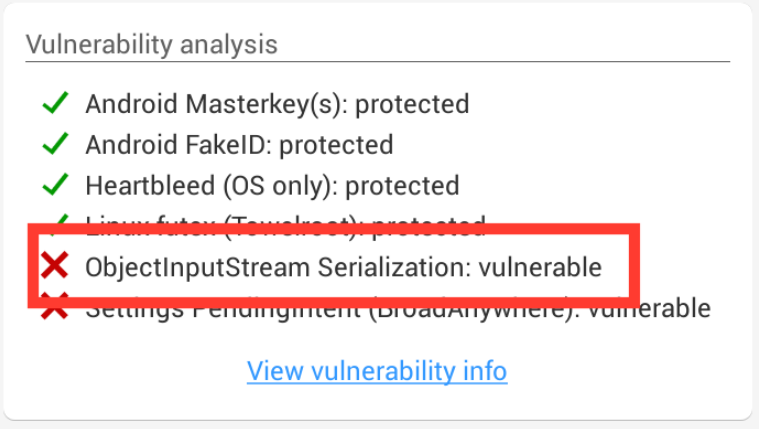
To determine if there was a trend in which devices have been patched or not, we analyzed the data collected by our app, Trustable by Bluebox. Trustable by Bluebox scans Android devices for mobile vulnerabilities and insecurities, including CVE-2014-7911. The app provides users with a Trust Score – a measure of security of the device – as well as which vulnerabilities their device is susceptible to and guidance on how to improve their overall security posture.

Our analysis found that about 20 percent of the manufacturers seen have issued a patch for CVE-2014-7911 to at least one of their devices running an Android OS before 5.0. This includes top manufactures like Samsung, HTC, Sony, LG, and Motorola. Some notable devices that we observed that are still running an OS before 5.0, but that are patched against CVE-2014-7911 are Blackphone and OnePlus One. Take a look at the screenshots below to see how Trustable by Bluebox identifies the ObjectInputStream Serialization vulnerability.

Not vulnerable:



Vulnerable:

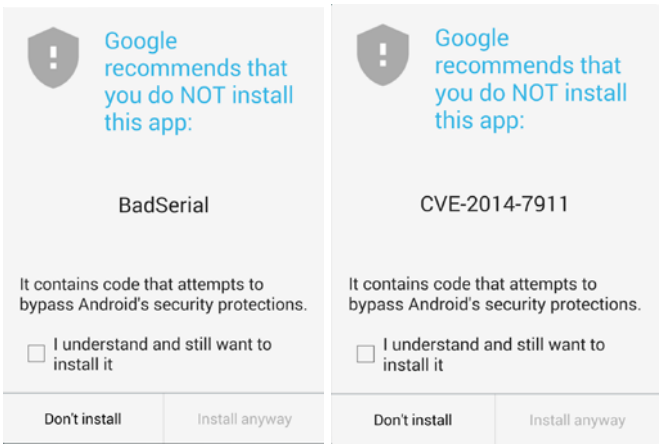


What is Google doing to protect users?

Android devices with Google Play installed have an option to verify the apps installed on the device. This is Google's attempt at a minimally invasive security scanner to warn against installing a known dangerous app that Google has flagged. Google is proactively checking for known insecure apps that exploit CVE-2014-7911.

While Google's scanner won't catch all apps that attempt to exploit it, Google has begun flagging the most popular ones. We discovered that Google has flagged at least two of the sample apps that are available online and provides a warning if you try to install an app that Google has identified as malicious.

A few examples below:



Some of the popular malware scanners will also identify these apps, but will also do what is called a deep scan to determine an application's behavior rather than solely relying on know bad apps. This means that these malware scanners will catch a wider pool of candidate apps that can attempt to exploit this vulnerability.

What can you do?

Use caution when downloading Android apps and be sure to download from reliable sources, like Google Play.Learn how trustable your device is, as well as discover if you are vulnerable to ObjectInputStream Serialization or others, by downloading Trustable by Bluebox for free in the Google Play Store: https://play.google.com/store/apps/details?id=com.bluebox.trust

About the Author

Andrew Blaich, Lead Security Analyst at Bluebox

Privacy Alert – Phone Charging Kiosks

At ChargeDefense, we continue to get looks of astonishment and outright fear when we explain the dangers of charging mobile devices through USB connections. Most people do not realize that when you plug your phone into a USB connection, the first thing that happens is an attempt by the device to synchronize with whatever it is plugged in to. Cyber criminals quickly recognized that this was an opportunity to exploit and use it to conduct identity theft and install malware on unsuspecting victims.

But, it's not just criminals that use USB connectivity to collect information from your mobile devices. Just like merchants and search engines install cookies on your computer to detect purchasing patterns and use that information to personalize targeted advertising just for you, your mobile devices can be used for the exact same thing. Your browsing history and purchasing patterns are valuable and that information can be collected and sold for profit. Your privacy is constantly in jeopardy.

One of the surprising tools used for collecting your personal information are public charging kiosks. We redacted an actual kiosk privacy policy agreement (you can't make this stuff up) to show you the true dangers of unprotected mobile device charging.

Information They Collect

When you connect to a public charging station such as the one in this example, you are effectively waiving your privacy rights. Their agreement terms (the fine print) states that it we ask for "personal and non-personal information" such as "name, address, phone number, credit card information, birthday, Facebook and/or Twitter usernames, and information regarding your cell phone and/or other mobile device."

The "agreement" goes on to state, "the Kiosk <Company> automatically receives and records information on our server logs from your browser or mobile platform". What are they automatically collecting?

Privacy Policy

Kiosk Privacy Policy

PLEASE READ THIS PRIVACY POLICY CAREFULLY BEFORE SUBMITTING ANY INFORMATION TO [redacted] OR THROUGH ANY [redacted] SOFTWARE OR KIOSK. BY SUBMITTING ANY INFORMATION YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND UNDERSTAND THIS POLICY AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF THIS PRIVACY POLICY, SIMPLY EXIT THIS PAGE AND/OR THE KIOSK SOFTWARE WITHOUT ACCESSING OR USING ANY OF OUR SERVICES.

2. Information We Collect.

There are several areas on the Website and/or within the Kiosk where you may be asked to enter both personal and non-personal information including, by way of example and without limitation, your name, address, phone number, credit card information, birthday, Facebook and/or Twitter usernames, and information regarding your cell phone and/or other mobile device. In addition, when you use the Kiosk [redacted] automatically receives and records information on our server logs from your browser or mobile platform, including your IP address and location [redacted] also collects and uses additional information from users such as transaction location, purchase activity, idle time, and all clicks and/or swipes within the Kiosk (together with time and order). We DO NOT sell or share any personal information about you to or with any person or organization except (i) as authorized by you, (ii) as set forth in the relevant portion of the Website, Kiosk or within any agreement between us, (iii) in connection with providing various products or Services to you (either directly or through one or more third parties), (iv) as may be required by law or court order, or (vi) as otherwise set forth herein. In particular, and not in limitation of the foregoing, information you enter at the Website and/or Kiosk (i) will be shared with the merchants or third party service providers with which [redacted] has entered into a business relationship in order to provide the Services, and (ii) may be shared with various third parties in connection with making available to you certain offers (which offers may be based on or related to your location at the time the offer is made available to you). In addition, [redacted] may sell, disclose or otherwise use information gathered on the Website or within the Kiosk to third parties on an aggregated basis.

- IP address and location
- Transaction location
- Purchase activity
- Idle time
- All clicks and/or swipes

What They Do With Your Personal Information

What are they doing with this information? Well, they TELL you they are sharing it with merchants and third party service providers they have partnerships with in order to target you with advertising.

3. How Your Information Is Used.

We use the information you provide to provide the applicable Services to you, either directly or through third party service providers, as further described above in this Privacy Policy. [redacted] may also share certain aggregated data with other third parties for general research, marketing and demographic purposes; however, this data, when shared on an aggregated basis, does not include any of your personal identifying information. Some of our Services may be offered in conjunction with partner companies, affiliates or other companies or websites with which we work. In order for us to provide these Services to you, it may be necessary for us to share your personal information with one of such entities. These parties are not allowed to use

What If I Don't Want Them To Collect My Personal Information?

I can never do a story without a little sarcasm, so here it is . . . Luckily, this particular vendor has a solution.

Business Transfer

We may, in the future, sell or otherwise transfer some or all of our assets or equity to a third party. Your personally identifiable information and other information we obtain from you via the Website or the Kiosk may be disclosed to any potential or actual third party purchasers of such assets or equity and may be among the assets transferred.

Acceptance

If you do not agree to the terms of this Privacy Policy, please do not provide us with any information and do not use the Website or the Kiosk. **By using the Website or the Kiosk and voluntarily providing information to us, you consent to our collection and use of the information as set forth in this Privacy Policy.**

You got it. First, they tell you they reserve the right to do whatever they want with your personal information in the future. Then they give you the out by telling you that if you don't want us to collect your information, then don't use our kiosk.

Conclusion

Your personal information is valuable and it is yours. There has been a disturbing trend where personal information is being collected and harvested by all kinds of people for all kinds of reasons. Some are somewhat benign, such as targeting personalized advertising. Some are much more

sinister such as identity theft and spying. Many people are either unaware or just accept it. And it is nearly impossible to avoid all of it since we all leave digital footprints when we purchase products and services, pay taxes, and live in communities. There is a digital record of all of us somewhere. We all like to think that those records are safe and being kept private. And, most organizations do have privacy policies in place and genuinely do care about protecting your privacy.

Some of these public charging kiosk companies obviously do not care about privacy and glibly state it in their policy. Unfortunately, sometimes you simply have no choice – you need to charge that phone and your only choice is the conveniently-located charging kiosk. ChargeDefense provides you with another solution. The Juice-Jack Defender® is guaranteed to block all data sharing at public charging kiosks – and beyond! So, when you are out and about, stick a charge cable and a Juice-Jack Defender® in your pocket or your purse wherever you go and protect your personal privacy.

About the Author

Stuart McCafferty

Like us on FaceBook and get special discount deals: www.facebook.com/chargedefense

Role of Government in Cyber Security

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids - This tremendous and confident dialogue announced by The President of the USA Mr. Barack Obama at 2015 State of the Union. It shows a hidden message of combating against cyber threats. Before few days, even UK Prime Minister David Cameron has expressed concern on cyber attacks against large companies and ensured them about "Cyber attack, war games" that will be acted with the USA in a cooperative manner towards cyber defense. Evolving cyber crime has opened the eyes of the governments of the globe, compelled them to take immediate steps to defense people and organizations.

(**Image Credit:** http://www.bbc.com)

The Average Cost of Cyber Crime:

If we look at the average cost of cybercrime in 2014 has crossed $12 million for organizations in the United States, which is 9% hiked up than the previous year 2013. The mostly attacks can be classified into web based attacks, phishing attack, social engineering, DDoS attack and malicious code.

Based on the global talk, we have three clear scenarios:

- It is clear to the government that cyber attacks are real and embryonic problematic. At some stage, foreign government is involved in actuating them.
- Cyber crime is bigger than we are scaling it and still not found the scope of cyber crime.
- Cyber threat requires more global efforts and tough defense strategies to mitigate it.

How the Government can participate?

Now the question is what organization, people, and above all the government can do to lessen the impact of cyber crime. Fewer steps in the direction of cyber defense from the government side can help a lot people & enterprises against developing cyber threats.

Governments must make a start on three front ends to support enterprise, by taking more lively approach against cyber attacks:

- Encourage a broader understanding of the business risk.
- Recognize and deal with the cultural aspects of the issue.
- Engage academia and businesses in formulating a mutual response.

Encourage a Broader Understanding of the Business Risk:

Many businesses do have a lack of understanding about the extent of the reach of cyber crime and its impact. A huge part of major company's value seems insubstantial and vulnerable to cyber threats. Even information assets and physical assets are probably vulnerable against cyber attack. Recent cyber attacks have shown us that weakness in physical and information asset, which can bring drastic damage to organizations. Therefore, measuring and determining individual business risk can make a great impact on business revenue, it is an effective way to disclose threats to IT management. To encourage businesses, a non-technical language can give confidence in recognizing, discoursing, and addressing the risks that companies face.

Recognize and Deal with the Cultural Aspects of the Issue:

Domestic approach to cyber issues, intellectual property rights, and fair competition plays a major role in forming cyber culture. There should be encouragement in building a strong security culture within the business and employees; they should be aware of protecting the corporate information by playing an active role in their job. There should be a balanced approach between control and liberty in cyberspace. Government should understand that cyber attacks are carried out by young talented personalities. Their skills should be realized as a part of the nationwide response to cyber attack and make them realize about their responsibilities toward society.

Engage Academia and Businesses in formulating Mutual Response:

Government can encourage collaboration with private sectors, universities, and international countries for better response against cyber threats by sharing the information with them and make confident about revealing security concerns to the government. Government can collaborate with universities as they can identify and develop talented hackers to build a defensive program against cyber attacks. Even government can join hands with other countries to share their data, which help to identify and understand the cybercrime in a practical manner.

Besides the above steps, there are a few suggestions that could really help businesses to diminish the cybercrime as well making individuals aware of it.

- The Government should build effective and single point access to report cyber crime and enhance the level of local police response for cyber victims.

- Even on social media, newly emerged frauds or threats should be addressed across different social media users, which can avert them from being victims of cyber crime.
- Motivate, support, and expand cyber security education at all levels, including critical key abilities, research, & development.
- Build a sole trustworthy point of counselling for the public and SMBs to help them remain safe online.
- The government should reduce vulnerabilities in its own national infrastructure and systems.
- Enhance the ability to protect and discourage high-end, state-sponsored threats and make sure these techniques are out of reach to non-state actors.
- Around 80% attacks can be mitigated by spreading security awareness among individuals and organizations, the government must work to raise awareness by educate and empower them.
- Law enforcement must have the proper tools to examine, interrupt and act against cyber crime.
- The existing relationship between the law enforcement and federal agencies should be improved and work cooperatively.
- Simplify and regulate the cyber breach reporting for businesses into a single federal law to make easy for customers and businesses.
- The federal, state, and local governments along with the private sector should work with a unity of effort to speed up progress in the area of cyber crime.

Conclusion:

After the announcement of Mr. Barack Obama on cyber security legislation, the whole world got a new hope for the progress in meliorating the nation's security. It is a wise step towards protecting innocent individuals and organizations against cyber threats. One person cannot task this responsibility, but every person of nation should do this. Even CNCI (Comprehensive National Cybersecurity Initiative) has rolled out goals and initiative to regulate Cyber Security defensive measures for today's emerging threats. To avert dangers to national security, Military infrastructure has designed some guidelines. This shows participation of Military in building national Cyber Security more fastened. With the combine efforts of the private sector, government enterprises, and individuals, we can make a safe cyber world of tomorrow.

About the Author

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

2015: Year of the RAT Threat Report Supplement

Defending Against Spear Phishing, RAT Deployment and Email Tracking

In my 2015: *Year of the RAT Threat Report (*see: http://www.snoopwall.com/reports/), I described how I felt Sony Pictures Entertainment (SPE) was attacked by the Guardians of Peace aka #GOP. In this supplement, I would like to cover how Spear Phishing works as well as Email Tracking, even commercial tools that are freely available for trials or limited email sending, which allow the sender to collect very useful data on the recipient including that which hackers typically use to exploit a common vulnerability and exposure (CVE, see: http://cve.mitre.org of which I serve on the Board and its sister search engine site http://nvd.nist.gov, funded by the US Department of Homeland Security to allow you, for free, to track and find any vulnerabilities in your network equipment, computer, operating system and software that might be used to exploit you).

Finding and Exploiting Vulnerabilities

It works like this – first you need to find email servers with vulnerabilities (CVEs) and then exploit them to eavesdrop upon and track others emails. This will then allow you to build up a contact list and what kind of messages a person sends, receives and opens, thus allowing you to spoof a trusted party and attach a remote access Trojan (RAT). I'm not telling you this to recommend you commit crime – in fact, I'm 100% against you doing so. However, without understanding why and how you might become a victim of a Spear Phishing attack with an embedded RAT attachment, or even exploitation of vulnerabilities in your email client or web browser, how can you expect to defend yourself? Just watch http://map.ipviking.com and you'll see loads of attacks against EMAIL SERVERS in the USA. Why? Because the first step in reconnaissance (RECON) for a spear phishing attack, is to break into a mail server, or find a recipient you can victimize so that you can later spoof an email to their important friend, boss or business associate that is your ultimate target.

What is the difference between Spear Phishing and Email Tracking?

Typically Spear Phishing are very targeted attacks going after one individual. Usually, email tracking is used by marketeers to make sure you opened an email they sent you and to collect additional information about you. Lately, due to the proliferation of free email tracking offerings, anyone from a debt collector to your local dentist or attorney or even a jealous spouse might use email tracking services to 'check up on you' which includes GEOLOCATION technology, now.

Email tracking generally will use a hidden cookie and a web bug (also known as a web beacon) to track the email. Spear Phishing will usually attach a RAT to the email hoping you will trust the spoofed sender and open the attachment, then causing a much more painful and deeper infection that may go unnoticed until it's too late, as in the case of Sony Pictures Entertainment.

Email tracking will tell the person tracking the email when an email was received, opened, and forwarded. It can tell when attachments or hyperlinks were opened and clicked. It can determine how long someone was reading the email. It can also collect information about the geolocation of

where it was opened. In addition they can find out about your computer operating system and the email client or web browser you are using to read the email.

Email tracking is used by individuals, email marketers, spammers, hackers, cyber criminals and phishers, to verify that emails are actually read by recipients, that email addresses are valid, and that the content of emails has made it past spam filters. When used maliciously, it can be used to collect confidential information about businesses and individuals and to create more effective phishing schemes. Most likely email tracking was employed with a spear phishing attack on Sony Pictures to learn what kind of environment they had inside their network and then to attack them with a Remote Access Trojan (RAT) through email.

There are dozens of email tracking companies and software to choose from with leading companies including icontact, constant contact, didtheyreadit, getresponse, activecampaign, interspire, getnotify, mxhero, litmus to yesware and so many more. Now anyone can afford email tracking because most sites off either a limited free account or free trial. On the limited free accounts you can only send so many tracking emails each day but they are completely free. Others offer a trial period such as 7 day free trial.

Is Email Tracking Creepware?

Email tracking can be considered #CREEPWARE because if you don't inform the recipient of your privacy policy, they may not know they are a victim of being eavesdropped upon. On the other hand for business purposes the argument is that you don't have to send a followup email and annoy someone to see if they opened your email or read it. The business argument is that you will learn how to better communicate with your customers.

What other ways are we being tracked?

Email tracking is only a part of the tracking process. Most folks have smartphones with apps that track them in even creepier ways every day. Companies that want to track you will use your email and your apps on smartphones and tablets plus search engines and social media sites like facebook and others will continue to expand their invasive eavesdropping on our behavior. The fact that email tracking is free and easy for anyone to try out and use, means it will probably continue to grow as another tracking arrow in the marketing or creepware quiver.

Beyond normal marketers, spammers, hackers, cyber criminals and phishers, some folks including spouses might use this method to make sure their spouse is where they say they are and some companies, including HP used it to make sure Board members weren't leaking information to the press or wall street analysts. Even investigators, attorneys, skip tracers for debtor or fugitive tracking and collection companies are using this tool to track people down.

Most people don't realize how our emails are being tracked. They simply open their emails, read them, ignore them or delete them and move on to the next email. Most people don't have antispam technology enabled and many of these emails get passed spam and antivirus filters. I think it's creepy for folks to use email tracking, even if it passes legal muster, without at the bottom of each of these emails, informing the recipient and offering them an opt out option. Privacy is good for

business and job seekers should also show they respect the privacy of the recipient, especially someone who might consider hiring them. This is alarming if a predator or stalker or spouse or x-spouse uses email to track you for their own creepy reason.

While Spear Phishing is Illegal, is Email Tracking Legal?

It is legal to track email. There are rules about spam and there are rules about bugging and eavesdropping on conversations but not about email. It's always best to disclose that you're using tracking tools to make sure the email gets to the right recipient and so that you won't have to bother them to see if they received and opened it.

However, here's where it gets real creepy. Imagine a stalker was trying to find out where you lived. If you opened their email, they could start to collect geolocation information on you as well as the 'fingerprint' of your computer and/or email client. This is the first part of a smarter attack known as spear phishing – they might use this to then find the right malware to attack your operating system or email or web client to install a RAT – a remote access Trojan, which is even more creepy software to watch you on your webcam and listen to you on your microphone.

If you want to legally and legitimately use email tracking for marketing or other purposes, I recommend folks put together a very positive and honest privacy policy or privacy statement in the bottom of these tracking emails so the recipients don't become victims.

How can you tell it's a Spear Phishing or Email Tracking Attack?

If it's an email that doesn't look like it contains a picture, usually the tracking cookie is an invisible picture – so by turning off 'display images' automatically, is the first hint. If you simply use TEXT only mode to read your emails instead of HTML, you'll know right away. If there's an attachment you were not expecting or if it seems 'fishy' it's probably a Spear Phishing attack. If you find a tiny white graphic that's one pixel in size, it's usually an Email Tracking attack. However, Spear Phishing attacks may also use this technology but they haven't in the past because it tips of the victim.

Defending Against Both Spear Phishing and Email Tracking Attacks

What is the simplest thing you can do to defend against this kind of attack? Change your email client settings to only display TEXT instead of HTML emails. When the email arrives, it might not look as pretty but you can still read it. If the entire email is a picture you know it's spam or email tracking. You won't enjoy missing the pretty colors, HTML hyperlinks, graphics and attachments but simple TEXT ONLY email is the answer. You simply cannot be victimized if you only read the text portion of the email message. That means an email client or special plug-in that renders the email as text only. Good news on major email clients such as Microsoft ® Outlook – all you have to do is change your security settings and you can make sure all hyperlinks are turned into text, all emails are read as text only and attachments are rejected.

This may start out making your day difficult, where you would then ask folks to send you attachments in a different fashion, but then you know it's really from them. For example, unless and

until DropBox, Filesanywhere, Box or similar services get hacked (which does happen from time to time…so be aware and stay vigilant), you can tell all your friends, coworkers and business associates you only accept attachments in a DropBox type service. I wouldn't recommend using Apple iCloud, Amazon Cloud, Microsoft Cloud Drive or Google Cloud Drive as they are targeted by hackers daily. Look for a less known service that offers encryption and stronger guarantees. Then, when someone is going to send you a file, tell them – don't use email, send it to this link (you provide them a way into your DropBox) and then before opening any of these attachments, you download them and then run them through your favorite antivirus scanner. If you are serious about security, run it through one of these:

http://www.virustotal.com which has over 40 different antivirus scanners that it runs on your file upload to determine if it's malware.

https://www.metascan-online.com/ which has currently 42 different antivirus scanners and like virustotal will accept file uploads that are over 100mb if need be to be scanned for detection of malware.

http://virusscan.jotti.org/en which has been around for a while only accepts 25mb file size uploads and quickly runs them through about 22 antivirus scanners to check for malware.

It's time we treat privacy respectfully. It's good for people and for businesses to be respectful to others right to privacy. If you want to track an email tell the recipients you are using email tracking technology. Sure, it can be a 4 point font at the bottom of the email but at least you're being honest about it. And for folks worried about their privacy, only receive emails in a TEXT viewing mode and you'll be safe. Consider this one more lesson we've learned from the Sony Pictures Entertainment breach.

Getting More Proactive and One Step Ahead of the Next Threat

As I said recently on BNN in Canada, see: http://www.bnn.ca/News/2015/1/24/How-businesses-can-neutralize-cyber-security-threats-in-2015.aspx entitled *Go Phish: The Rise of Hacking – Part Three*, the biggest threats we face this year are:

- Spear phishing (targeted email) attacks
- Remote Access Trojans (RATs) which are used to control a computer in another location
- Mobile Devices loaded with eavesdropping malware in the form of trusted and free apps

It's time consumers, small offices – home offices (SOHOs) and small to medium sized businesses (SMBs) as well as large enterprises get more proactive and assume you already have vulnerabilities and malware. Start with:

- Training employees better
- Hardening systems
- Detecting and removing RATs
- Deploying full disk encryption and real-time backups
- Defending against phishing attacks
- Managing the BYOD (Bring Your Own Device) dilemma

If you're an SMB or Enterprise, you should take the following steps right away before you become the next victim:

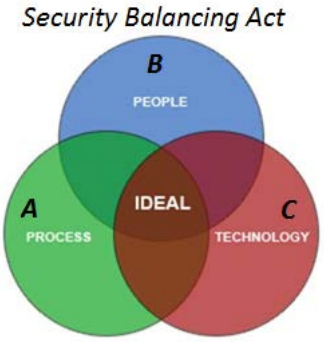
- Educate employees against social engineering and phishing attacks.
- Make sure you encrypt computers, hard drives, databases and all the data.
- Make sure you enforce better password management policies.
- Run and test frequent backups and disaster recovery plans.
- Create and manage corporate security policies around the standards such as ISO 27001 or COBIT.

About The Author

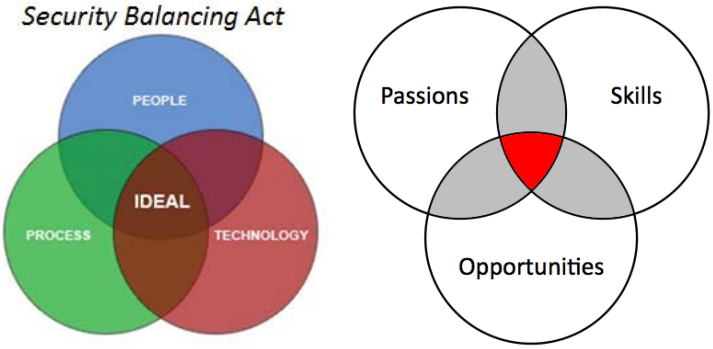
Gary is the CEO of SnoopWall and inventor of the company's new Counterveillance technology. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine and the cover story author and regular contributor to Hakin9 Magazine. He also founded NetClarity, Inc.,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

The Security Balancing Act: People – Process – Technology

Everyone in IT and Security has seen the "People, Process, and Technology – (PPT)" Venn diagrams that depict the ideal state that enterprises are striving to achieve.



Instead of just looking at a PPT diagram alone – let's also look at a Venn diagram depicting the ideal state that employees want to achieve in their place of employment – their career.



The two diagrams when overlaid suggest that for an organization to achieve an ideal state of security, the organization's associates need to be able to achieve an ideal state within their career. After many years in the IT Security industry, I find the most effective security practices involve a balance of all three disciplines for an organization to succeed. The definition of success from organization to organization may vary but in principle it is focused on the following:

- Engaged associates
- Brand protection
- Market share protection
- Consumer confidence

In order for the security balancing act to be successful, organizational processes must be sound. In addition, the technology must be relevant to the business process, and people must be informed

and educated. If any one of the PPT disciplines is overly used within an organization the result could be failure – which in turn will impact an organization's brand, market share, consumer confidence, and their associates negatively. No matter how many security layers a server is protected by, and how locked down a server may be by policy – all it takes is one (1) associate who has access to the server to write their password on a sticky note and post the note on their monitor – don't laugh – I have seen it done time and time again – even in the most secure facilities in the world.

If organizations have no process in place to guide their associates or the technology implemented on the correct actions and activities to take to be secure – how will the organization be secure? Ultimately – they will fail at being secure.

Understanding that the three PPT disciplines are different from one another allows an organization to start building the right tactical and strategic approaches for each discipline to be successful within their organization focused on achieving their organization's ideal state. Here are a few challenges and suggestions that I have encountered over the years for each PPT discipline that may help you on your organizations ideal state journey:

A – Process / Organizational

Challenges:

- Security requirements, rules, and policies are weak, not aligned with industry best practices, or undefined
- Insecure operations, daily procedures not defined or not well defined
- No disaster recovery, business continuity, or break the glass procedures defined

Suggestions to overcome / solve these challenges:

- Share, Communicate, Document, Explain (SCDE)
- Enforce controls, policies, and procedures
- Automate where possibly *only* where it makes business sense
- Understand that high-risk procedures are not always the best procedures for automation

B – People / Associates / Human

Challenges:

- Lack of understanding of real business risks and threats
- Managers and Senior leaders have little involvement with defining Information Systems Security Policies for the organization
- A culture that rewards thoughtlessness, carelessness, neglect, passivity, irresponsibility
- A culture of IT security shaming

Suggestions to overcome / solve these challenges:

- Communicate and inform associate, manager, and Senior leaders with security awareness campaigns focused on do behavior as opposed to don't behavior
- Enforce automatic controls where possible and ensure notifications of enforcement are received by key business stake holders
- Follow basic rules and common-sense security measures both practical and pragmatic in nature
- Do not reject security policies when a business impact occurs – learn and adjust
- Build a strong partnership between business and IT to avoid misperceptions and misunderstandings

C – Technology / Technical

Challenges:

- Design weakness: identify software, architecture, engineering, and security requirements late / post production
- Security exploits not identified prior to deployment
- Bug or misconfiguration on a system which can be used by an attacker (internal / external) to gain unauthorized access
- Business perception of Technology improvements impacting business operations

Suggestions to overcome / solve these challenges:

- Include security, audit, risk, and compliance in all projects; from the minor tactical ones to the most strategic ones
- Audit, review older projects and implementations to avoid unknown security risks
- Implement tools to prevent malware, exploits, and over entitled / access definitions for people
- Enforce the organizations change management procedure
- Align technology to the business NOT business to the technology

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.

Two-factor authentication with Security Key

By Dean Wiech

Google recently introduced a new log in technique that uses a USB stick that would provide an even stronger protection for particularly security-sensitive individuals. And it's not just any USB stick — the company claims it will replace the use of the traditional password and username to log in to a system. The so called Google Security Key is a physical USB second factor that only works after verifying the log in site is truly a Google website, not a fake site pretending to be Google. Rather than typing a code, the user inserts the Security Key into the computer's USB port and taps it when prompted in Chrome.

To facilitate this, Google supports the U2F standard, a multi-factor authentication technique intended to offer users enhanced security. Multi-factor or two-factor authentication involves logging in with something you know (password), and something you own (a smartphone, token, biometrics or USB stick). For instance, users could use a password to log in; they then receive a four-digit code on their mobile phones that they are prompted to input. Google's Security Key works according to the same principle, but slightly different. It eliminates the possibility of phishing, a risk that is still present with verification codes received on a smartphone.

However, another, perhaps easier, form of two-factor authentication is to log in using a combination of an access badge and a PIN code. Many companies offer their employees access to their premises with an access badge, which can be conveniently used for log in procedures, but also for self-service printing or payment in the company's restaurant. After placing the access badge on a card reader and entering a PIN code, users gain access to the network. Since they already have the badge in their possession, in my view, it would be easier to use this log in technique rather than provide employees with yet another additional device, in this case, in the shape of an USB stick – doing so only means they will have one more "device" to manage.

If organizations combine the access badge/PIN code approach with single sign-on at the point of log, employees and the organization are ensured a secure and user friendly experience at the same time. Why? Because a single sign-on solution enables end users to log in just once after which access is granted automatically to all of their authorized applications. If you want to facilitate a secure login, SSO can be used a as medium of exchange for your end users.

Regarding card readers, you may say: But card readers also comprise additional hardware. And you would be right. In fact, a card reader also is a USB device that allows employees the ability to use their access badge as an additional authentication factor. However, the benefit that a card reader has over a USB stick is that the card reader does not have to support any type of encryption, meaning it cannot be hacked.

About the Author

Dean Wiech is managing director of Tools4ever, a global supplier of access and identity management solutions.

INFOSEC WORLD 2015

Conference & Expo

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

Cyber Defense Magazine readers save 10%!

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

WWW.MISTI.COM/INFOSECWORLD

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

SnoopWall

RECLAIM YOUR PRIVACY ™

Introducing PrivacyShield™

Your Last Line of Defense to Protect Your Mobile Customers and Mitigate Risk

The high risk behaviors of mobile device users expose banks to an extensive variety of malware, data leakage, and fraud liability.

Banks have the liability & ID Fraud losses associated with insecure mobile devices and careless consumer behavior.

The "last mile" in mobile banking security lies not on your security efforts, but on the security of your customer's mobile smartphone and other wireless devices.

Increasing mobile banking app security is both a challenge and an opportunity for your bank, and the customer retention, operational cost savings and fraud reduction should make it a priority.

Russian Hackers Amass Over a Billion Internet Passwords

The New York Times
AUG. 5, 2014

"90% [of the apps from 40 of the top 60 Banks] contained several non-SSL links...[this] allows an attacker to....create a fake login prompt or similar scam."

Ariel Sanchez, IOActive, Jan 14, 2014

48% of consumers say they will not use mobile banking services due to security concerns

- The Risk & Rewards of Mobile Banking Apps
Webroot, 2014

www.snoopwall.com sales@snoopwall.com

SnoopWall

RECLAIM YOUR PRIVACY ™

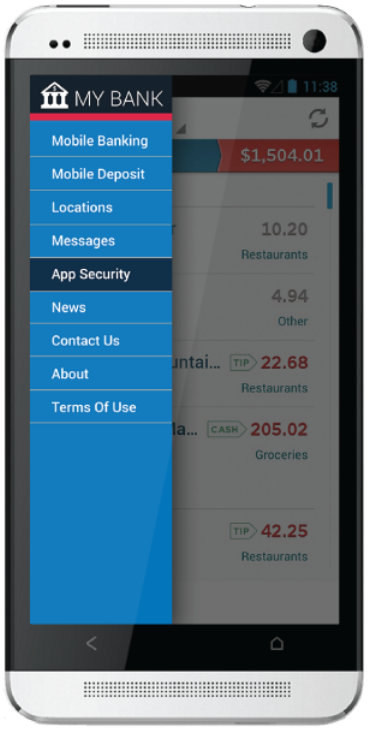
SnoopWall® Privacy Shield™ - an embedded Security Solution for Mobile Banking Applications

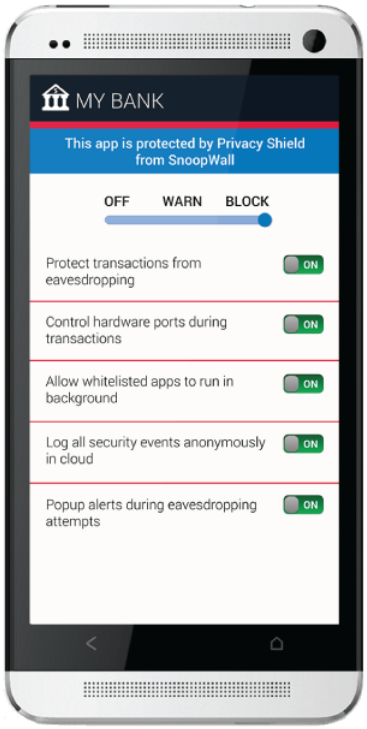
SnoopWall® has discovered serious vulnerabilities in existing mobile banking apps which expose Customers' Personal Identifiable Information (PII).

SnoopWall® Privacy Shield™ Embedded is our powerful, patent-pending counterveillance engine designed to protect customers' PII and sensitive financial information, shielding transactions from eavesdropping by apps you might have trusted, but are malicious.

Privacy Shield™ Embedded intelligently controls access to ports which pose security/privacy vulnerabilities.

- Acts like a firewall for mobile banking apps
- Designed to be embedded in mobile apps
- Shields financial information from eaves dropping
- Fixes vulnerability gaps left behind by AV, Authentication etc.
- Powerful, yet transparent to consumers





Provides a secure environment for Mobile financial transactions

For more information about how you can protect the last line of defense in your mobile banking transactions, please visit **www.snoopwall.com** or call **(800) 991-3871 x1000.**

About SnoopWall
SnoopWall is the world's first counterveillance software company focused on helping consumers and enterprises protect their privacy on all of their computing devices including smartphones, tablets, and laptops.

One Tara Boulevard, Suite 200
Nashua, NH 03062
(603) 821-4704

Platform Support:

Windows 7 or higher Apple iOS 7 or higher Android 2.4 or higher

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

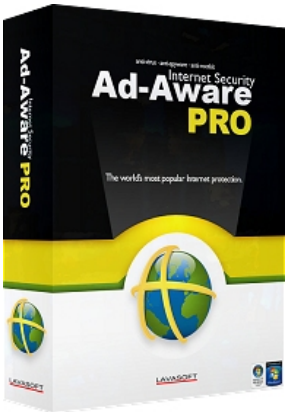
Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

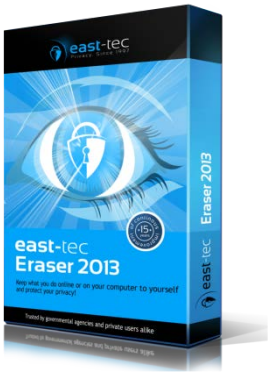
Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

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.





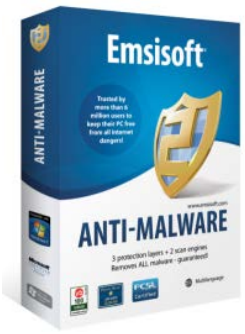
So use it by going here:

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 February 2015

Sample Sponsors:

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

Cyber Warnings Newsflash for February 2015

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

Unknown "device" lands on White House grounds; no danger seen
http://in.reuters.com/article/2015/01/26/usa-whitehouse-device-idINKBN0KZ0V120150126

CyberPatriot Reveals Top 28 Teams Advancing to National Finals Competition
http://www.prnewswire.com/news-releases/cyberpatriot-reveals-top-28-teams-advancing-to-national-finals-competition-300025297.html

The Seven Types of Cybercriminals
http://www.slate.com/articles/news_and_politics/crime/2015/01/cybercrime_manhattan_district_attorney_cyrus_vance_says_there_is_a_tsunami.html

NSA reform still cyber bill's biggest hurdle
http://thehill.com/policy/cybersecurity/230601-nsa-reform-remains-cyber-bills-biggest-hurdle

Obama, Congress may find cybersecurity consensus
http://www.usatoday.com/story/news/politics/2015/01/25/cybersecurity-information-sharing-bill/22229049/

Independent assessment gives VA's cybersecurity positive mark
http://www.federalnewsradio.com/1177/3787774/Independent-assessment-gives-VAs-cybersecurity-positive-mark

True cybersecurity: 'Intelligent' computer keyboard identifies users by pattern of their key taps
http://www.washingtontimes.com/news/2015/jan/24/true-cybersecurity-intelligent-computer-keyboard-i/

Adobe updates Flash Player again, plugs 0-day exploited by Angler
http://net-security.org/secworld.php?id=17867

NIST Revises Crypto Standards Guide
http://www.govinfosecurity.com/nist-revises-crypto-standards-guide-a-7831

Google discloses three severe vulnerabilities in Apple OS X
http://www.cnet.com/news/google-team-finds-three-severe-vulnerabilities-in-apple-os-x/

Thousands of US Gas Stations Vulnerable to Remote Hacks
http://threatpost.com/thousands-of-us-gas-stations-vulnerable-to-remote-hacks/110608

DOJ fears tech 'zone of lawlessness'
http://thehill.com/policy/technology/230840-doj-fears-tech-zone-of-lawlessles

Facebook takes blame for service outages, which hit wider Web
http://www.reuters.com/article/2015/01/27/us-facebook-down-idUSKBN0L00GE20150127

Self-destructing chat app Wickr uses cat pics to hide photos in plain sight
http://www.engadget.com/2015/01/27/wickr-timeline-cat-pics/

F.T.C. Calls for Strong Data and Privacy Protection With Connected Devices
http://bits.blogs.nytimes.com/2015/01/27/f-t-c-calls-for-strong-data-and-privacy-protection-with-connected-devices/?_r=0

Today: Congressional cyber double-header - Internet of Things in FTC spotlight - First Look: More grim statistics about DDoS
http://www.politico.com/morningcybersecurity/0115/morningcybersecurity16876.html

Maldrone: Malware which hijacks your personal drone
http://www.zdnet.com/article/maldrone-malware-which-hijacks-your-personal-drones/

Supposedly clean Office documents download malware
http://www.net-security.org/malware_news.php?id=2947

Security Is a Must for the Internet of Things
http://recode.net/2015/01/27/security-is-a-must-for-the-internet-of-things/

Singapore ups the ante in cyber security fight
http://www.reuters.com/article/2015/01/27/us-singapore-cybersecurity-idUSKBN0L011T20150127

Cybersecurity savant
http://thehill.com/business-a-lobbying/business-a-lobbying/230796-cybersecurity-savant

U.S. FCC warns against blocking personal Wi-Fi access
http://www.cnbc.com/id/102375201#.

China crackdown makes it harder to get around the Great Firewall
http://money.cnn.com/2015/01/28/technology/china-censorship-vpn-great-firewall/

RansomWeb: Crooks Start Encrypting Websites And Demanding Thousands Of Dollars From Businesses
http://www.forbes.com/sites/thomasbrewster/2015/01/28/ransomweb-50000-dollar-extortion/

Advocates want to hear from AG nominee on Aaron Swartz
http://thehill.com/policy/technology/230967-advocates-want-lynch-to-answer-questions-on-aaron-swartz

Dutch judge approves hacking suspect's extradition to US
http://www.washingtontimes.com/news/2015/jan/27/dutch-judge-approves-hacking-suspects-extradition-/

'Ghost' flaws poses high risk to Linux distributions
http://www.computerworld.com/article/2875780/ghost-flaws-poses-high-risk-to-linux-distributions.html

Barriers to Passing Federal Breach Notification Bill
http://www.govinfosecurity.com/barriers-to-passing-federal-breach-notification-bill-a-7847

NIST Publishes Guide to Mobile Apps Vetting
http://www.govinfosecurity.com/nist-publishes-guide-to-mobile-apps-vetting-a-7839

NIST Revises Crypto Standards Guide
http://www.govinfosecurity.com/nist-revises-crypto-standards-guide-a-7831

NFL Mobile App Leaks Unencrypted Credentials
http://threatpost.com/nfl-mobile-app-leaks-unencrypted-credentials/110694

Ultra-secure Blackphone Vulnerability lets Hackers Decrypt Texts
http://thehackernews.com/2015/01/blackphone-vulnerability.html

You won't be able to fly this hugely popular drone in D.C. much longer, thanks to that White House crash
http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/28/a-simple-software-update-could-have-prevented-a-drone-from-buzzing-the-white-house/?hpid=z14

Regin super-malware has Five Eyes fingerprints all over it says Kaspersky
http://www.theregister.co.uk/2015/01/28/malware_bods_find_regin_malware_reeks_of_warriorp

ride/

Lynch vows to 'expand and enhance' DOJ's cyber work
http://thehill.com/policy/cybersecurity/231008-lynch-vows-to-expand-and-enhance-dojs-cyber-work

China puts cybersecurity squeeze on US technology companies
http://www.theguardian.com/technology/2015/jan/29/china-puts-cybersecurity-squeeze-on-us-technology-companies

The Next Step in the Cybersecurity Plan
http://science.dodlive.mil/2015/01/28/the-next-step-in-the-cybersecurity-plan/

China accused of protectionism through new cybersecurity rules aimed at western tech companies
http://9to5mac.com/2015/01/29/china-tech-protectionism/

Is data privacy just a dream?
http://www.cnet.com/news/is-data-privacy-just-a-dream/

D-Link routers vulnerable to DNS hijacking
http://net-security.org/secworld.php?id=17888

Drones crash onto White House agenda
http://thehill.com/policy/technology/231096-drones-crash-on-to-white-house-agenda

Guidance to improve risk management and IoT
http://net-security.org/secworld.php?id=17890

Hacker's List: This 'Hire A Hacker' Site Must Be A Joke, A Scam Or Just Sucks
http://www.forbes.com/sites/thomasbrewster/2015/01/29/hackers-list-is-really-bad/

China Says It Wants 'Downwards Trend' In Censorship - While Blocking VPNs
http://www.forbes.com/sites/emmawoollacott/2015/01/30/china-says-it-wants-downwards-trend-in-censorship-while-blocking-vpns/

Watchdog: Attkisson wasn't hacked, had 'delete' key stuck
http://thehill.com/policy/technology/231225-doj-watchdog-ex-cbs-reporter-wasnt-hacked-had-delete-key-stuck

Report disputes claims that US hacked reporter's computer
http://www.washingtontimes.com/news/2015/jan/29/report-disputes-claims-that-us-hacked-reporters-co/

Taking Security Training to the Next Level
http://www.govinfosecurity.com/interviews/taking-security-training-to-next-level-i-2559

Seeking Compromises on CyberSec Bills
http://www.govinfosecurity.com/blogs/seeking-compromises-on-cybersec-bills-p-1804

Be warned: Google enlists Chrome in push for encrypted Web
http://www.cnet.com/news/chrome-becoming-tool-in-googles-push-for-encrypted-web/

ZeroAccess Click-Fraud Botnet Back in Action Again
http://www.darkreading.com/zeroaccess-click-fraud-botnet-back-in-action-again/d/d-id/1318865?

Why Iran Hacks
http://www.darkreading.com/perimeter/why-iran-hacks/a/d-id/1318862?

Department of Energy CIO Says Digital Drive Must Not Be Stunted By Cyber Threats
http://www.forbes.com/sites/gauravsharma/2015/01/30/department-of-energy-cio-says-digital-drive-need-not-be-stunted-by-cyber-threats/

Singapore to Open Cybersecurity Agency
http://www.govinfosecurity.com/singapore-to-open-cybersecurity-agency-a-7859

Gazing Into the Cyber Security Future: 20 Predictions for 2015
http://www.govinfosecurity.com/whitepapers/gazing-into-cyber-security-future-20-predictions-for-2015-w-1290

Brazil: The Global Fraud Test Kitchen
http://www.govinfosecurity.com/interviews/brazil-global-fraud-test-kitchen-i-2562

D-Link routers vulnerable to DNS hijacking
http://www.net-security.org/secworld.php?id=17888

New spy case shows Russia up to old tricks, prosecutors say
http://www.stripes.com/news/us/new-spy-case-shows-russia-up-to-old-tricks-prosecutors-say-1.327104

Raspberry Pi 2 - $25 Computer with Quad-Core Processor and it runs Free Windows 10
http://thehackernews.com/2015/02/Raspberry-Pi-2-windows-10.html

Beware of malware on smartphones
http://digital.asiaone.com/digital/news/beware-malware-smartphones

Data risks give rise to 'cyber insurance' policies
http://www.desertsun.com/story/money/business/2015/02/01/cyber-insurance-hackers/22682675/

US Army Releases Cyber-Forensic Code to Github
http://www.infosecurity-magazine.com/news/us-army-releases-cyberforensic/

AG nominee Lynch expected to be fighter on cyber crime
http://thehill.com/policy/cybersecurity/231335-ag-nominee-lynch-expected-to-be-fighter-on-cyber-crime

Cyber crime threat stalks fund houses
http://www.ft.com/cms/s/0/b1d5725a-a7af-11e4-be63-00144feab7de.html#axzz3QaaKsal2

Cyber gets $1B boost in White House budget
http://thehill.com/policy/cybersecurity/231449-cyber-gets-1-billion-boost-in-white-house-budget

Obama budget dedicates $14B to cybersecurity
http://www.washingtontimes.com/news/2015/feb/2/obama-budget-dedicates-14b-to-cybersecurity/

Spies seek $3 billion budget boost
http://thehill.com/policy/technology/231465-spies-want-budget-boost

Syrian Rebels Hacked Via Skype
http://www.govinfosecurity.com/syrian-rebels-hacked-via-skype-a-7863

China Demands Tech Companies to give them Backdoor and Encryption Keys
http://thehackernews.com/2015/02/iphone-china-backdoor.html

Cyber crime is a threat to global economy, says researcher
http://www.computerweekly.com/news/2240239300/Cyber-crime-is-a-threat-to-global-economy-says-researcher

BMW Update Kills Bug In 2.2 Million Cars That Left Doors Wide Open To Hackers
http://www.forbes.com/sites/thomasbrewster/2015/02/02/bmw-door-hacking/

Windows 10 Installs Automatically On Windows 7 And Windows 8
http://www.forbes.com/sites/gordonkelly/2015/02/02/windows-10-automatic-install/2/

An Avatar That Busts Pedophiles Goes on Autopilot
http://www.bloomberg.com/news/articles/2015-02-02/an-avatar-that-busts-pedophiles-goes-on-auto-pilot

Murdoch's Fox, News Corp. Won't Be Charged Over Hacking
http://www.bloomberg.com/news/articles/2015-02-02/murdoch-s-fox-news-corp-won-t-be-charged-in-u-s-for-hacking

Revenge-porn website operator convicted in San Diego
http://www.washingtontimes.com/news/2015/feb/3/revenge-porn-website-operator-convicted-in-san-die/

Google Adds Research Grants to Bug Bounty Program
http://threatpost.com/google-adds-research-grants-to-bug-bounty-program/110800

DNS Hijack in D-Link Routers, No Authentication Required
http://threatpost.com/dns-hijack-in-d-link-routers-no-authentication-required/110792

New Adobe Flash 0-Day Used In Malvertising Campaign
http://www.darkreading.com/new-adobe-flash-0-day-used-in-malvertising-campaign/d/d-id/1318900?

Browsers Are The Window To Enterprise Infection
http://www.darkreading.com/browsers-are-the-window-to-enterprise-infection/d/d-id/1318906?

WebRTC Vulnerability leaks Real IP Addresses of VPN Users
http://thehackernews.com/2015/02/webrtc-leaks-vpn-ip-address.html

Mobile Threat Monday: SaveMe Malware Infiltrates Google Play
http://securitywatch.pcmag.com/mobile-security/331685-mobile-threat-monday-saveme-malware-infiltrates-google-play

Digital Evidence Requires an Understanding of 'Cyberlaw'
http://www.forensicmag.com/news/2015/02/digital-evidence-requires-understanding-cyberlaw

WH creates 'E-Gov Cyber' unit to oversee agency security
http://thehill.com/policy/cybersecurity/231598-white-house-creates-e-gov-cyber-unit

White House Creates Cyber Governance Unit Within OMB
http://threatpost.com/white-house-creates-cyber-governance-unit-within-omb/110831

White House readies cyber executive action
http://thehill.com/policy/cybersecurity/231633-white-house-readies-cyber-executive-action

Administration Modifies Data Collection Rules
http://www.govinfosecurity.com/administration-modifies-data-collection-rules-a-7871

Malware targets users seeking info on Islamic State group

http://www.japantimes.co.jp/news/2015/02/04/national/crime-legal/malware-targets-users-seeking-info-islamic-state-group/#.VNIOB2M4erM

New Technology Detects Hacks in Milliseconds
http://www.bloomberg.com/news/articles/2015-02-03/new-technology-detects-hacks-in-milliseconds

Microsoft Internet Explorer Universal Cross-Site Scripting Flaw
http://thehackernews.com/2015/02/internet-explorer-xss.html

New Banking Trojan Targets Android, Steals SMS
http://threatpost.com/new-banking-trojan-targets-android-steals-sms/110819

New Wave of CTB-Locker/Citroni Ransomware Hitting Victims
http://threatpost.com/new-wave-of-ctb-lockercritroni-ransomware-hitting-victims/110820

1,800 Domains Overtaken By Flash Zero Day
http://threatpost.com/1800-domains-overtaken-by-flash-zero-day/110835

Jeremy Hammond, Anonymous hacker, put on terrorist list by FBI
http://www.washingtontimes.com/news/2015/feb/3/jeremy-hammond-anonymous-hacker-put-on-terrorist-l/

Google Trades Technicality For Brevity With New SSL Warning
http://threatpost.com/google-trades-technicality-for-brevity-with-new-ssl-warning/110842

China to ban online impersonation accounts, enforce real-name registration
http://www.reuters.com/article/2015/02/04/us-china-internet-censorship-idUSKBN0L80ZF20150204

Enterprises Underestimate Actual Shadow Cloud Risks
http://www.darkreading.com/cloud/enterprises-underestimate-actual-shadow-cloud-risks/d/d-id/1318941?

3 Disturbing New Trends in Vulnerability Disclosure
http://www.darkreading.com/3-disturbing-new-trends-in-vulnerability-disclosure/d/d-id/1318925?

Silk Road Creator Faces Overwhelming Evidence
http://www.forensicmag.com/news/2015/02/silk-road-creator-faces-overwhelming-evidence

Admin alert: Twice as many digital certificates used to sign malware reported in 2014
http://www.firstpost.com/business/admin-alert-twice-many-digital-certificates-used-sign-malware-reported-2014-2078619.html

Dyre banking trojan tweaked to spread Upatre malware via Microsoft Outlook
http://www.networkworld.com/article/2878966/microsoft-subnet/dyre-banking-trojan-tweaked-to-spread-upatre-malware-via-microsoft-outlook.html

"Exploit This": Evaluating the exploit skills of malware groups
https://nakedsecurity.sophos.com/2015/02/03/exploit-this-evaluating-the-exploit-skills-of-malware-groups/

News Flash! 3rd time unlucky! New 0-day hits Adobe's browser plug-in...
https://nakedsecurity.sophos.com/2015/02/03/news-flash-3rd-time-newunlucky-0-day-hits-adobes-browser-plug-in/

Jeffrey and Mary Archer settle phone-hacking claim
http://www.theguardian.com/uk-news/2015/feb/04/jeffrey-and-mary-archer-settle-phone-hacking-claim

Health insurance giant Anthem hit with major data breach
http://thehill.com/policy/cybersecurity/231832-health-insurance-giant-hit-with-major-data-breach

Siemens ICS Switches Hit With Buffer Overflow, Authentication Bugs
http://threatpost.com/siemens-ics-switches-hit-with-buffer-overflow-authentication-bugs/110852#sthash.As6cuhHc.dpuf

Defense nominee: US 'not where it should be' on cybersecurity
http://thehill.com/policy/cybersecurity/231781-defense-nominee-us-not-where-it-should-be-on-cyber

Latest Flash 0Day Under Attack; Possible Ties to Group Behind Angler EK
http://threatpost.com/latest-flash-0day-under-attack-possible-ties-to-group-behind-angler-ek/110847#sthash.40Gx0snv.dpuf

House bill would ban mandated tech access
http://thehill.com/policy/cybersecurity/231745-house-reintroduces-bill-to-ban-tech-backdoors

IE Memory Attacks Net ZDI $125,000 Microsoft Bounty
http://threatpost.com/ie-memory-attacks-net-zdi-125000-microsoft-bounty/110876#sthash.s6gQymJf.dpuf

Jury Finds Ross Ulbricht Guilty of Running Silk Road Marketplace
http://www.forbes.com/sites/sarahjeong/2015/02/04/jury-finds-ross-ulbricht-guilty-of-running-silk-road-marketplace/

Congress takes another swing at ending warrantless reading of email
http://www.computerworld.com/article/2880125/congress-takes-another-swing-at-ending-

warrantless-reading-of-emails.html

New spyware steals pictures and data from iOS devices
http://www.computerworld.com/article/2879089/new-spyware-steals-pictures-and-data-from-ios-devices.html

Backblaze releases raw data on all 41,000 HDDs in its data center
http://www.computerworld.com/article/2879994/backblaze-releases-raw-data-on-all-41000-hdds-in-its-data-center.html

Confide for business users lets you share sensitive docs that then disappear
http://www.computerworld.com/article/2879670/confide-for-business-users-lets-you-share-sensitive-docs-that-then-disappear.html

Scan Finds 'Ghost' Haunting Critical Business Applications
http://www.darkreading.com/vulnerabilities---threats/scan-finds-ghost-haunting-critical-business-applications/d/d-id/1318975?

Espionage Campaign targets iOS devices with Malware apps
http://thehackernews.com/2015/02/malware-espionage-ios-apps.html

Army Cyber Defenders Open Source Code
http://science.dodlive.mil/2015/02/04/army-cyber-defenders-open-source-code/

Malware alert: If you downloaded these 3 Android apps, remove them immediately

http://www.digitaltrends.com/mobile/google-removes-adware-app-from-google-play/

Report compares exploit skills of APT actors, other malware groups
http://www.scmagazine.com/researcher-looks-at-attacker-exploit-skills/article/396487/

Cyber crime poses greater risk to SMEs, warns Ernst & Young expert
http://www.irishexaminer.com/business/cyber-crime-poses-greater-risk-to-smes-warns-ernst-young-expert-310833.html

Chinese State-Sponsored Hackers Suspected in Anthem Attack
http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

Groups Urge U.S. Fight Against China Foreign Tech Purge
http://www.bloomberg.com/news/articles/2015-02-06/business-groups-urge-u-s-fight-against-china-foreign-tech-purge

Obama Taps VMware IT Executive as Federal CIO

http://www.govinfosecurity.com/obama-taps-vmware-exec-as-federal-cio-a-7883

Who's Hijacking Internet Routes?
http://www.govinfosecurity.com/whos-hijacking-internet-routes-a-7874

The World's Email Encryption Software Relies on One Guy, Who is Going Broke
http://www.forensicmag.com/news/2015/02/worlds-email-encryption-software-relies-one-guy-who-going-broke

Better open source hygiene would have spooked GHOST
http://www.networkworld.com/article/2880598/security0/better-open-source-hygiene-would-have-spooked-ghost.html

USF opens new center to fight cybercrime
http://www.mynews13.com/content/news/cfnews13/news/article.html/content/news/articles/bn9/2015/2/6/usf_opens_new_center.html

Your Samsung SmartTV Is Spying on You, Basically
http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html

Is this the future of cyberwarfare?
http://america.aljazeera.com/watch/shows/america-tonight/articles/2015/2/5/blackenergy-malware-cyberwarfare.html

Govs need not break encryption to beat cybercrime
http://www.cbronline.com/news/security/govs-need-not-break-encryption-to-beat-cybercrime-4505483

Crowdsourcing America's cybersecurity is an idea so crazy it might just work
http://www.washingtonpost.com/blogs/innovations/wp/2015/02/05/crowdsourcing-americas-cybersecurity-is-an-idea-so-crazy-it-might-just-work/

DARPA: Cyberattacks against US military 'dramatically increasing'
http://thehill.com/policy/cybersecurity/232122-darpa-official-cyberattacks-against-us-military-dramatically-increasing

Senate leader calls for US government's explanation in wake of HSBC leaks
http://www.theguardian.com/news/2015/feb/09/hsbc-senate-democrat-us-government-biggest-leak

Samsung admits its Smart TV is spying on you
http://thehackernews.com/2015/02/smart-tv-spying.html

Hacktivist Group Anonymous (#OpISIS) Takes Down Islamic State (ISIS) Social Media Accounts
http://thehackernews.com/2015/02/anonymous-isis-cyber-attack.html

Beware of Fake 'WhatsApp Web' Spreading Banking Tojan
http://thehackernews.com/2015/02/whatsapp-web-malware.html

4 open-source monitoring tools that deserve a look
http://www.networkworld.com/article/2880113/network-management/4-open-source-monitoring-tools-that-deserve-a-look.html

How the NSA is improving security for everyone
http://www.networkworld.com/article/2880477/security0/how-the-nsa-is-improving-security-for-everyone.html

Cyber insurance: You better shop around, says EY's Robert Reeves
http://www.techrepublic.com/article/cyber-insurance-you-better-shop-around-says-eys-robert-reeves/

Adware Medic Removes Macintosh Malware
http://lifehacker.com/adware-medic-removes-macintosh-malware-1684264260

US Government builds "Memex Deep Web Search Engine" to track criminals
http://thehackernews.com/2015/02/memex-deep-web-search-engine.html

Anthem Breach: Phishing Attack Cited
http://www.govinfosecurity.com/anthem-breach-phishing-attack-cited-a-7895

FFIEC Issues Cyber-Resilience Guidance
http://www.govinfosecurity.com/ffiec-issues-cyber-resilience-guidance-a-7893

Modern cars are ripe targets for hackers
http://gulfnews.com/business/technology/modern-cars-are-ripe-targets-for-hackers-1.1454379

Car Makers Aren't Being Honest On Hacker And Privacy Threats
http://www.forbes.com/sites/thomasbrewster/2015/02/09/car-makers-wont-admit-cyber-problem/

Researcher Releases 10 Million Usernames And Passwords In Fight Against Obama's War On Hackers
http://www.forbes.com/sites/thomasbrewster/2015/02/10/10-million-passwords-published-fight-against-obama-war-on-hackers/

Obama to unveil cyber data-sharing unit
http://thehill.com/policy/cybersecurity/232235-obama-to-unveil-intel-community-cyber-unit

Wall Street regulator weighing insurance industry cyber rules
http://thehill.com/policy/cybersecurity/232209-wall-street-regulator-weighing-insurance-cyber-rules

5 technologies that betrayed Silk Road leader's anonymity
http://www.computerworld.com/article/2881755/5-technologies-that-betrayed-silk-road-leaders-anonymity.html

Julian Assange 24hr guard leaves London police with £10m bill
http://www.theguardian.com/media/2015/feb/10/julian-assange-guard-london-police-10m-bill-ecuadorian-embassy

Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm
http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025?

KickAss Torrent download website seized
http://thehackernews.com/2015/02/torrent-website-kickass-seized.html

Government Contract to Grier Forensics Speeds-Up Digital Investigation
http://www.forensicmag.com/articles/2015/02/government-contract-grier-forensics-speeds-digital-investigation

Selfie With Body Leads to Murder Suspect
http://www.forensicmag.com/news/2015/02/selfie-body-leads-murder-suspect

Cyber Attacks Rising Around Utah NSA Facility
http://www.forensicmag.com/news/2015/02/cyber-attacks-rising-around-utah-nsa-facility

'Glaring hole' in Australia's cyber security policy
http://www.theage.com.au/it-pro/security-it/glaring-hole-in-australias-cyber-security-policy-20150209-139h8n.html

Custom Linux malware used in brute-force attacks
http://www.gmanetwork.com/news/story/431396/scitech/technology/custom-linux-malware-used-in-brute-force-attacks

Security Researcher Releases 10 Million Sets Of Username-Password To The Public Domain
http://en.yibada.com/articles/13061/20150211/security-researcher-releases-10-million-set-username-password-public-domain.htm

Court upholds NSA snooping
http://thehill.com/policy/technology/232385-court-upholds-nsa-snooping

Obama urges 'swift work' on cyber issues in call with Chinese leader
http://thehill.com/policy/international/232413-obama-urges-swift-work-on-cyber-issues-in-call-with-chinese-leader

U.S. states want Anthem to provide hack info quickly to customers
http://www.computerworld.com/article/2881937/us-states-want-anthem-to-provide-hack-info-quickly-to-customers.html

Microsoft tightens leash on POODLE attacks against IE11
http://www.computerworld.com/article/2882351/microsoft-tightens-leash-on-poodle-attacks-against-ie11.html

Cryptowall 3.0 Slims Down, Removes Exploits From Dropper
http://threatpost.com/cryptowall-3-0-slims-down-removes-exploits-from-dropper/110923

Chinese Hacking Group Codoso Team Uses Forbes.com As Watering Hole
http://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059?

Box Giving Customers Control Over Encryption Keys
http://www.darkreading.com/box-giving-customers-control-over-encryption-keys/d/d-id/1319028?

Google hands out free Drive space for running quick security checklist
http://www.networkworld.com/article/2882553/network-storage/google-hands-out-free-drive-space-for-running-quick-security-checklist.html

eDiscovery tools and methodologies can "significantly enhance" digital forensic investigation: UK Home Office report
http://www.businesswire.com/news/home/20150210005942/en/eDiscovery-tools-methodologies-%E2%80%9Csignificantly-enhance%E2%80%9D-digital-forensic#.VNtMfGM4erM

TurboTax Fraud May Impact Federal Returns Too, FBI Investigating
http://www.forbes.com/sites/robertwood/2015/02/12/turbotax-fraud-may-impact-federal-returns-too-fbi-investigating/

Three of Tech's Top CEOs to Skip Obama Cybersecurity Summit
http://www.bloomberg.com/news/articles/2015-02-11/three-of-tech-s-biggest-ceos-to-skip-obama-cybersecurity-summit

Republican senator pushes bill to require warrants for emails
http://thehill.com/policy/technology/232586-hatch-pushes-bill-to-require-warrants-for-emails

'Anonymous' hacking group shuts down over 800 Islamic State Twitter accounts
http://www.washingtontimes.com/news/2015/feb/11/anonymous-hacking-shuts-800-islamic-state-sites/

Microsoft Group Policy Vulnerability Affects All Windows Computers
http://threatpost.com/microsoft-group-policy-vulnerability-affects-all-windows-computers/110990

Experts Warn 2015 Could be 'Year of the Healthcare Hack'
http://www.forensicmag.com/news/2015/02/experts-warn-2015-could-be-year-healthcare-hack

DARPA Hones Skills of Future Cyber Officers
http://www.forensicmag.com/news/2015/02/darpa-hones-skills-future-cyber-officers

Govt admits cyber attacks, but says can't identify culprits
http://indianexpress.com/article/india/india-others/govt-admits-cyber-attacks-but-says-cant-identify-culprits/

Security engineers are playing Russian roulette with alerts: Damballa
http://www.zdnet.com/article/security-engineers-are-playing-russian-roulette-with-alerts-damballa/

Facebook fights cybercrime: Social network launches threat network for security experts to clamp down on hackers

http://www.dailymail.co.uk/sciencetech/article-2950473/Facebook-fights-cybercrime-Social-network-launches-threat-network-security-experts-clamp-hackers.html

White House goal: Kill the password
http://thehill.com/policy/cybersecurity/232684-white-house-goal-kill-the-password

Obama set for cyber push
http://thehill.com/policy/cybersecurity/232729-obama-set-for-cyber-push

Anarchist hackers start cyber war with ISIS
http://thehill.com/policy/cybersecurity/232583-anarchist-hackers-go-to-cyber-war-with-isis

Jeb Bush's email cache held another surprise: Old computer viruses
http://www.computerworld.com/article/2883804/jeb-bushs-email-cache-held-another-surprise-old-computer-viruses.html

Facebook fixes flaw that could have let hackers delete photos
http://www.computerworld.com/article/2883735/facebook-fixes-flaw-that-could-have-let-hackers-

delete-photos.html

Google boss warns of 'forgotten century' with email and photos at risk
http://www.theguardian.com/technology/2015/feb/13/google-boss-warns-forgotten-century-email-photos-vint-cerf

Lack of CSPRNG Threatens WordPress Sites
http://threatpost.com/lack-of-csprng-threatens-wordpress-sites/111016

Bypassing Windows Security by modifying 1 Bit Only
http://thehackernews.com/2015/02/bypassing-windows-security.html

The Great Bank Heist, or Death by 1,000 Cuts?
http://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts/

Bank Hackers Steal Millions via Malware
http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0

Carnegie Mellon response team has battled computer virus attacks since 1988

http://triblive.com/news/editorspicks/7693096-74/computer-attacks-pittsburgh#axzz3RvBBRmg4

Lizard Squad is back: group 'attacks Xbox Live and Daybreak Games'
http://www.theguardian.com/technology/2015/feb/16/lizard-squad-attacks-xbox-live-daybreak-games

How Cyber-security Leaders Evaluate White House Strategy
http://www.eweek.com/security/how-cyber-security-leaders-evaluate-white-house-strategy.html

Obama Signs Information-Sharing Executive Order To Boost Cybersecurity: How Effective Will It Be?
http://www.techtimes.com/articles/32911/20150216/obama-signs-information-sharing-executive-order-boost-cybersecurity-effective-will.htm

White House Hosts Summit on Cybersecurity
http://www.toptechnews.com/article/index.php?story_id=1000034M9RC8

1 billion data records compromised in data breaches
http://net-security.org/secworld.php?id=17954

Did Obama's Cyber Summit Miss the Mark?
http://www.govinfosecurity.com/did-obamas-cyber-summit-miss-mark-a-7918

This $150,000 Kickstarter Campaign Wants To Turn Kids Into Crime Scene Investigators
http://www.forbes.com/sites/thomasbrewster/2015/02/17/kickstarter-for-csi-kids/

Vladimir Drinkman Pleads Not Guilty In 160 Million Credit Card Hacking Case
http://www.forbes.com/sites/katevinton/2015/02/17/vladimir-drinkman-pleads-not-guilty-in-160-million-credit-card-hacking-case/

Code typo helps tie North Korea to the Sony hack
http://www.computerworld.com/article/2885534/code-typo-helps-tie-north-korea-to-the-sony-hack.html

Cybercrime Gang: Fraud Estimates Hit $1B
http://www.govinfosecurity.com/crime-gang-fraud-estimates-hit-1b-a-7916

APT Groups Emerging in Middle East
http://threatpost.com/apt-groups-emerging-in-middle-east/111124

Encryption and Silence Can be Targets' Best Assets
http://threatpost.com/encryption-and-silence-can-be-targets-best-assets/111131

Bank Hackers Steal Millions With Malware
http://www.forensicmag.com/news/2015/02/bank-hackers-steal-millions-malware

Army Reserve Partnership Aims to Grow Cyber Warriors
http://www.forensicmag.com/news/2015/02/army-reserve-partnership-aims-grow-cyber-warriors

Password Cracking Experts Decipher Equation Group Crypto Hash
http://www.forensicmag.com/news/2015/02/password-cracking-experts-decipher-equation-group-crypto-hash

How Lenovo's Superfish 'Malware' Works And What You Can Do To Kill It
http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-need-to-know/

See How This Android App Clones Contactless Credit Cards In Seconds
http://www.forbes.com/sites/thomasbrewster/2015/02/18/android-app-clones-cards/

White House: Clock ticking on cyber sharing
http://thehill.com/policy/cybersecurity/233143-white-house-has-4-years-to-get-cyber-relations-right

MegaNet - New Decentralized, Non-IP Based and Encrypted Network
http://thehackernews.com/2015/02/meganet-decentralized-internet.html

The Possible Put Into Digital Forensic Practice With Grier Technology

http://www.forensicmag.com/articles/2015/02/possible-put-digital-forensic-practice-grier-technology

Desert Falcon Group Swooped on One Million Files
http://www.forensicmag.com/news/2015/02/desert-falcon-group-swooped-one-million-files

AccessData Launches Free 20-Day Trial Program for Digital Forensics Products
http://globenewswire.com/news-release/2015/02/18/707503/10120624/en/AccessData-Launches-Free-20-Day-Trial-Program-for-Digital-Forensics-Products.html

Android malware spies on you even after phone is shut down
http://mashable.com/2015/02/19/android-malware-spies-shut-down/

Digging Deeper: Inside the forensics laboratory of officer who leads child pornography investigations
http://www.kttc.com/story/28144772/2015/02/18/digging-deeper-inside-the-forensics-laboratory-of-officer-who-leads-child-pornography-investigations

It's time for a National Cybersecurity Safety Board (NCSB) - Opinion
http://www.csoonline.com/article/2886326/security-awareness/it-s-time-for-a-national-cybersecurity-safety-board-ncsb.html

Privacy & Cybercrime Use The Same Tools
http://www.informationweek.com/partner-perspectives/bitdefender/privacy-and-cybercrime-use-the-same-tools/a/d-id/1319163

Drones, cybercrime among topics at annual AG meeting
http://legalnewsline.com/news/255013-drones-cybercrime-among-topics-at-annual-ag-meeting

Babar the Elephant: Another malware plague with a cute name
http://www.theregister.co.uk/2015/02/19/babar_french_cyberespionage/

The Company Behind Lenovo's Dangerous Superfish Tech Claims It's Under Attack
http://www.forbes.com/sites/thomasbrewster/2015/02/20/komodia-lenovo-superfish-ddos/

This one weird script continually crashes Android email
http://www.theregister.co.uk/2015/02/19/this_script_will_continually_crash_email_in_samsung_4_minis/

Managing technology in an unmanageable world
http://thehill.com/blogs/congress-blog/technology/233126-managing-technology-in-an-unmanageable-world

Officials: Cyber heist didn't hit US

http://thehill.com/policy/cybersecurity/233270-banking-officials-cyber-heist-didnt-hit-us

After high-profile hacks, many companies still nonchalant about cybersecurity
http://www.csmonitor.com/World/Passcode/2015/0219/After-high-profile-hacks-many-companies-still-nonchalant-about-cybersecurity

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

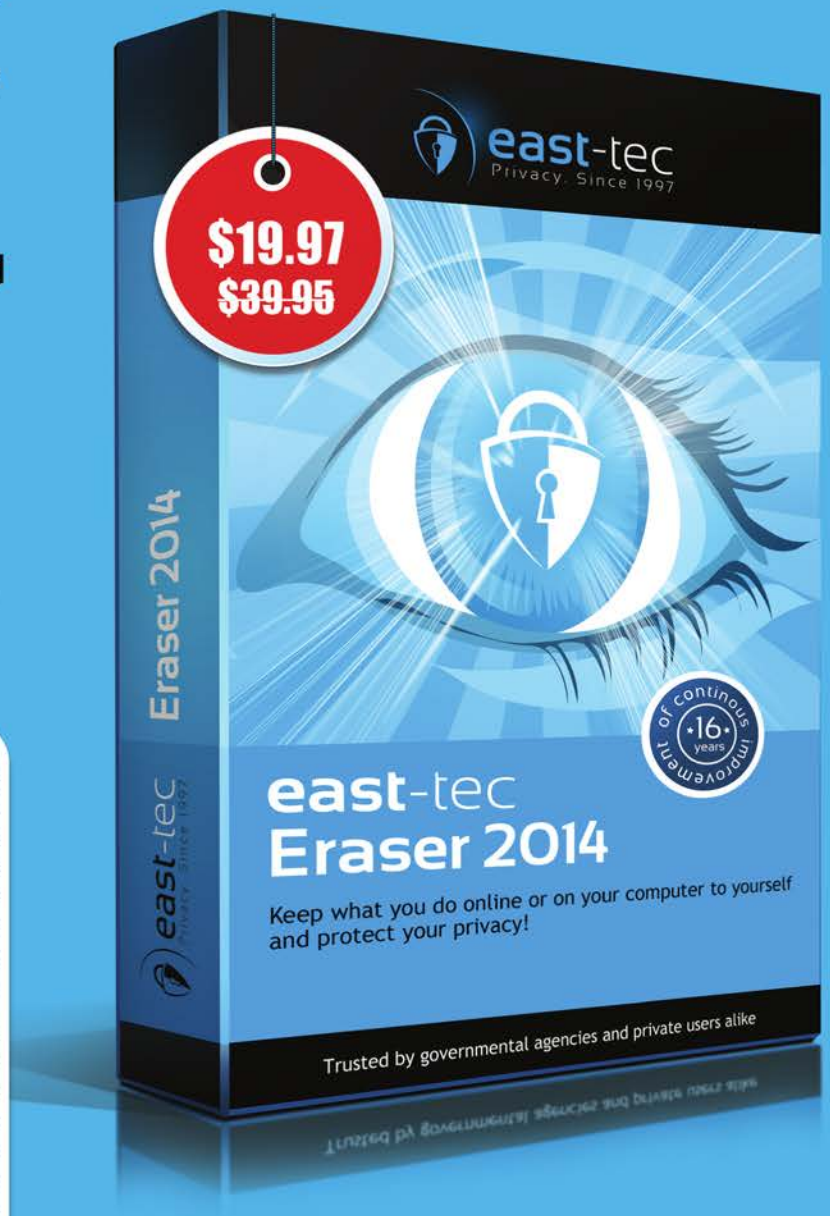
Cyber Defense Magazine - Cyber Warnings rev. date: 02/23/2015

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