CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

SEPTEMBER 2014

MORE INSIDE!

CONTENTS

Follow the Yellow Brick Road to Automation and Best Practices 2

Approach To Improving Cybersecurity And Critical Infrastructure Protection Must Include A Focus On The Basics 4

Hut, Hut, Hike: Ramp up Your Defenses Against Cyber Attacks 8

How an Aggressive Chinese IP Highlights Attribution Issues ... 12

The Top Ten Mobile Flashlight Applications Are Spying On You. Did You Know? 22

10 Architectural Principles that Prevent Code Modification or Reverse-Engineering 25

Using Automated Threat Response to Mitigate Security Events 28

Your Server as the Last Line of Cyber Defense 31

The CISOs struggle for respect in the enterprise 37

The Comprehensive Approach To Securing Websites 39

Malwarebytes' Growth Accelerates in Hot Anti-Malware Market 42

Briefly about Cyber Security Metrics 46

Best Security Practices for Data Recovery 50

Why the NGFW isn't enough 52

Your USB Device Can Contain Malware – How to Remain Safe 56

Today's Wolf of Wall Street: Electronic teeth and a bigger appetite 58

Does mobile increase security risk for EHRs? 60

Top 3 Myths About Antivirus Software 62

NSA Spying Concerns? Learn Counterveillance 63

Top Twenty INFOSEC Open Sources 64

National Information Security Group Offers FREE Techtips 65

Job Opportunities 66

Free Monthly Cyber Warnings Via Email 66

Cyber Warnings Newsflash for September 2014 69

CYBER WARNINGS

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats. Wizard of Oz clip used under fair use of the US Copyright Act.

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

PierLuigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Pierluigi Paganini
Bob Dix
Paula Skokowski
Tim O'Brien
Jonathan Carter
Paul Nguyen
Scott Schweitzer
Julian Waits
Matthias Chin
Gary Good
Milica Djekic
Michael Hall
Timothy Liu
Peter Davidson
Troy Gill
Jeff Forristal

and many more…

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Follow the Yellow Brick Road to Automation and Best Practices

As we head into the fall, I can't help but think about the Wizard of Oz. Deep inside the security of the Emerald City, Dorothy and her friends finally make it past the evil witch (malware), past the guards at the gates (firewall) and finally into the heart of the city (data center) where they meet the Wizard – I presume you are that Wizard.

If you are a cyber security expert or a CIO or an IT manager – if you are the champion of securityyou're your network, you have to play Wizard of Oz and create an image that you are 'magical' and 'bigger than life'. But in reality, behind the curtain you are really just like the rest of us – a fallable human with all the tools at your disposal to do the best job you can to impress others that your 'castle' is secure. In reality to truly be an IT Security Wizard, you have to build up strong defenses and get one step ahead of the next threat. This requires more than 'smoke and mirrors' but actual best practices and as much automation you can muster so you don't have to keep tinkering with the tools to create a 'projection' that you are the Wizard.

In this edition, we follow the Yellow Brick road and work our way down a path that is more challenging but the results should be an incredible information exchange where you gain knowledge from our expert writers in each area of infosec that needs best practices and as much automation as possible. Some of my favorite automation tools are intelligent alerts by taking the time to properly setup your Security Events Information Management (SEIM) system or patch, configuration and vulnerability management where one click gets many systems properly hardened and updated.

But even with the best automation, we still must practice what we preach. We need to review all aspects of INFOSEC to make sure we aren't missing a gap. The biggest gap I've found is in trusting and fallable humans. We're all so trusting. This opens doors to social engineering, remote exploitation and malicious insiders. If you don't train others to help you get one step ahead of the next threat, you'll be working your magic with 'smoke and mirrors' while the evil witch steals your crown jewels in your Emerald City.

To our faithful readers, there's no place like home, there's no place like home and CDM is ours, together,

Pierluigi Paganini

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

Approach To Improving Cybersecurity And Critical Infrastructure Protection Must Include A Focus On The Basics

Blocking and Tackling Will Move the Needle of Cyber Protection

By Bob Dix

While the government seems to be focused primarily on worst-case cyber scenarios—potential events with projected significant impact, but very low probability of happening—there is much more we as a nation of stakeholders in a globally connected community, could do to improve our overall cybersecurity and critical infrastructure profile.

As with physical security, it is important to recall that cybersecurity and critical infrastructure protection is about assessing and managing risk. It is not possible to protect everything all of the time.

There is no one-size-fits-all approach to cybersecurity. Risk management requirements, business or personal needs, and resource availability vary among a wide range of stakeholders, as do the approaches to assessing and managing cybersecurity risk. It all starts with awareness and education about the threats, vulnerabilities and consequences of engaging in cyberspace.

Accordingly, it is time to focus on fundamental steps that will improve our current cybersecurity and critical infrastructure protection profile, while thinking about and planning for more severe events. A holistic approach to this critical national and economic security issue will produce more effective and tangible results.

The following are examples of actionable steps that should be included as pieces of a blueprint for improving cybersecurity and critical infrastructure protection. In the past few months I have explained how IT supply chain security (May 2014) and proper cyber hygiene (July 2014) fit into this blueprint. Each of these actions can be pursued today and would improve our overall ability to defend against the growing threats in cyberspace.

The rhetoric must meet reality when it comes to the government's commitment to the public-private partnership for cybersecurity and critical infrastructure protection. Industry partners are *volunteers* that have contributed significant time, energy, and resources to support the partnership for many years. There is still significant room for improvement in achieving an equitable approach to true partnership, such as early engagement, jointly setting priorities, defined action steps, and measuring outcomes, particularly with regards the U.S. Department of Homeland Security (DHS). Far too often, DHS treats private sector owners and operators of this nation's critical infrastructure as a nuisance, not as partners. Successful engagement with the private sector is often characterized by DHS based only on how many meetings were held and how many people attended, as opposed to outcomes and actions that contributed to making the nation safer and more secure.

This is a regrettable situation as there is a *shared* responsibility for meeting the mission of improving the protection, security, and resilience of a wide range of stakeholders in cyberspace.

It appears that far too many people at DHS are more concerned about who is in charge rather than collectively advancing an environment of trust and collaboration to meet the challenge of the growing risk environment.

Sectors such as energy and financial services enjoy more productive partnerships. Perhaps there are lessons to be learned from these engagements that could be applied by DHS more broadly across the public-private partnership. More productive results will be achieved for the American people with an equitable and collaborative partnership.

A National Weather Service (NWS) for cybersecurity type model is necessary to provide timely, reliable, and actionable situational awareness for cybersecurity. Both the NWS and the Center for Disease Control provide models for creating an integrated operational capability that embraces the strengths of the public and private sectors in an environment of collaboration and trust. These models prove that in collaboratively utilizing technology and data analysis, we are capable of achieving timely, reliable, and actionable situational awareness. Such awareness permits the issuance of information such as alerts and warnings, and even recommended measures to proactively improve the detection, prevention, and mitigation of risks.

Such a capability does not exist for cybersecurity and critical infrastructure protection today, although the foundation for how to get there does exist. We need to seize the moment, leveraging a functional public-private partnership to achieve improved results for the American people.

The National Cybersecurity and Communications Integration Center (NCCIC), which according to the U.S. government serves as the nerve center for cybersecurity, is instead a series of stovepipes, including a collection of one-off agreements with individual companies and organizations. Some progress has been made with the NCCIC, but nearly five years after its creation, it remains a work in progress stymied by cultural impediments and a lack of collaborative leadership.

Creating an operational capability is more than pushing out threat indicators in volume and claiming victory. It must include information sharing, analysis, and collaboration across the partner community. The targeted outcome must be timely, reliable, and include actionable situational awareness, both in steady state and during times of escalation that can produce alerts, warnings, and even recommended protective measures. The NCCIC will achieve greater success if it leverages an integrated approach that includes industry, federal cyber centers and entities, state and local governments, along with our international allies. These efforts are essential to improving the detection, prevention, and mitigation of cyber events that may become incidents of national or even global consequence.

Leverage lessons learned from actual events and exercises intended to test our national preparedness and resilience. The government has a lot of information related to actual cyber events from around the world. Analyzing those events offers information about the tactics, techniques, and procedures (TTPs) utilized by the bad guys. Developing case studies based on these events would be very instructive to the cybersecurity community for managing risk to data, systems, networks, and critical infrastructure. In focusing on the TTPs the analysis should

explain how proper protective measures would have mitigated or reduced the impact of the event.

Regrettably, the U.S. government often cites actual event information as “classified” and therefore not eligible to be shared. Again, stakeholders are not focused on the sources and methods that often cause information to be classified. Sharing information about which TTPs were used and how those events might have been prevented would help raise the bar of education and awareness for stakeholders and practitioners.

Since 2006, the U.S. government has conducted a series of national cybersecurity exercises primarily through DHS and FEMA. These exercises focused on various scenarios and threats, have produced a variety of lessons learned and after action reports. However, as demonstrated during a recent review, little if any action has been taken on the items identified and documented, and many of the same items continue to appear in succeeding reports.

If we are going to invest in testing cyber readiness to identify gaps and then develop an improvement plan to address those gaps, it is difficult to understand how this valuable information seems to have been only minimally addressed.

The lessons learned and after action reports are valuable; therefore, someone should tackle the findings and demand answers as to what steps have been taken to address the documented gaps and weaknesses.

The legal environment governing cybersecurity, electronic crimes, and privacy includes legislation that was largely enacted during a predominantly analog world. The time for approaching the review of the legal environment in a piece meal manner has passed. There should be a comprehensive examination of the current laws and regulations to reflect the needs of a digital world, while promoting economic growth and providing privacy and protection of civil liberties.

Several pending pieces of legislation attempt to address important issues such as information sharing; timely, reliable, and actionable situational awareness; liability protection; and privacy. It is important to have a broader view of the entire legal framework governing cybersecurity and critical infrastructure protection.

The activities included in this blueprint are not exclusively intended to address the risks associated with attempted disruption of the electric grid by nation states or terrorist organizations; the supply of oil and natural gas; the water supply; or the transportation system. These are all-important considerations and should be evaluated in the context of risk management, including the potential impact and likelihood; the economics of cybersecurity; and the business and personal needs of constituent stakeholders.

Instead, the blueprint is intended as a practical approach to raising the bar for cybersecurity and critical infrastructure across a wide array of stakeholders and threats. By implementing these actions we can disrupt the tactical and economic model of the bad guys—whether they are

hackers, criminals, social and political dissidents, disgruntled insiders, nation states, or terrorist organizations.

The steps in this blueprint can have a meaningful impact as we work together in a joint, integrated, and collaborative manner to address an important element of the current risk environment that has the ability to touch all of us in some way. It is time for action that can improve our overall cybersecurity and critical infrastructure protection profile, and in doing so make our nation safe and more secure.

About the Author

Bob Dix is the Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks. Dix has enjoyed a distinguished career in both the public and private sector, and is widely recognized across industry and government as a subject matter expert and a leading policy expert in furthering government/industry partnerships to protect U.S. critical infrastructure.

Hut, Hut, Hike: Ramp up Your Defenses Against Cyber Attacks

By Paula Skokowski, CMO, Accellion

Fall is almost upon us. You know what that means: the kids are back in school, the leaves will soon turn colors and it's time for football. While I'm not someone who's glued to the TV every Sunday watching NFL games, I can't help but tune in to cheer on my local team. Go 49ers!

Therefore, when asked to provide my thoughts on how organizations can better protect themselves from cyber attacks, I couldn't help but think of parallels to the game. After all, one of IT's jobs is blocking and tackling internal and external security threats in order to keep confidential data safe and employees as productive as possible.

This is no small feat with data constantly on the move. According to Cisco's Global Mobile Data Traffic Forecast, there are seven billion mobile devices on the planet – almost the same number as there are humans. Plus, analyst firm, IDC estimates that over the next six years, 90 percent of new spending on Internet and communications technologies will be on cloud-based technologies – a whopping $5 trillion global business. It's no wonder we find ourselves being pulled in so many directions when it comes to proactively managing data security.

A comprehensive IT defense has more components than can be properly named in one article. I've outlined seven best practices to add to your defense playbook to keep your enterprise data out of unwanted hands in this fast-moving era of mobile and cloud computing.

1) *Don't underestimate your opponents:* You don't have to look far to find a headline on yet another cyber attack. Last December, the theft of 40 million credit card numbers at Target. Last month, the largest known data breach to date with a Russian crime ring stealing 1.2 billion usernames and passwords from 420,000 websites. And, just today, as I'm writing this, a hacking incident at JP Morgan Chase and several other financial institutions. If we've learned one thing over the past year it's that no one is immune. We need to continuously fine-tune and enhance our defenses because we cannot predict where the next malicious attackers will strike.

2) *Expand your cheering section:* Too often, cyber security management is left solely to IT. While IT should certainly drive many of the decisions, such as technology evaluations and purchases, data security initiatives require buy-in from senior management, compliance officers and employees. According to a report by Kroll and Compliance Week, three quarters of compliance officers have no involvement in managing cyber security risk. It's a good idea to hold regular security briefings with executives on new types of threats, as well as educational sessions for staff on risks and reminders about internal policies related to mobile computing. This will help the organization gain a greater understanding that protecting your intellectual property is critical to company's success.

3) *Think twice about that trade:* Far too often, IT hands over control of their enterprise data to a cloud provider, giving them full responsibility without completing understanding the risks. This puts the onus on the cloud vendor to care for your data as if it's their own – a huge responsibility

considering you're on the hook to meet regulatory requirements whether the information is stored within your company or with a third-party provider. A report by SkyHigh Networks – a company that tracks the use of cloud services for corporate customers – found that organizations used an average of 759 cloud services in Q1 2014 – a 21% increase over the previous quarter. The same report revealed that of the total amount of cloud services used in Q1 – 3,571 – only 7% were "enterprise-ready", meeting stringent requirements for data protection, identify verification, services security and legal protection. Make sure to do proper due diligence before selecting a cloud vendor to find out exactly where you data will reside, who has access and what controls are in place to keep breaches at bay.

4) *Stop the quarterback sneak:* When there's no easy way for employees to get to the documents they need, when they need them, they'll figure it out on their own. Short on time, employees will turn to the first public cloud file sharing service they can find, particularly if the solution is easier to use than what is available from their employer. This opens up huge security risks, particularly when IT isn't aware of the situation or intentionally turns a blind eye. It's important to endorse one file sharing solution and collaboration solution for use enterprise-wide. If you don't, employees will likely turn to consumer-class solutions and you lose control over how files are distributed and who has access.

5) *Promote teamwork:* You want to enable employees to easily access data without resorting to the file sharing workarounds discussed above. Therefore, it's critical to provide ubiquitous mobile access to data regardless of where it resides – in SharePoint, on shared drives, or ECM systems. You also want to provide integration with LDAP and Active Directory, as well as single sign-on services, DLP services and mobile device management (MDM) systems, for the peace of mind that security controls are consistent across all employees' communications.

6) *Don't forget that you're the coach:* Keeping pace with employees' mobile accessibility requirements doesn't mean you have to give up fine-grained control. You require around-the-clock visibility into file and data activity, including logging and audit trails to support compliance requirements. Remember that you call the shots and need to enforce your organization's own security, compliance and mobile access policies behind-the-scenes while keeping mobile workers productive.

7) *Prepare for the fumble:* Every 3.5 seconds someone in the U.S. loses a cell phone. Therefore, you need to make sure you have remote monitoring, logging and wiping capabilities to provide much-needed visibility and control should a device be lost or stolen.

You want to securely mobilize enterprise content and reap the rewards of cloud computing while keeping your company's data safe from unwanted eyes. The key is to find a winning strategy that builds upon your organization's existing security controls, provides secure access to any content from any devices from anywhere and enables employees to be as productive as possible.

About the Author

Paula Skokowski, Chief Marketing Officer, Accellion

Ms. Skokowski joined Accellion in February 2007. She has more than 20 years experience in product marketing, corporate marketing and new product introduction for pre and post-IPO companies in Silicon Valley. Prior to Accellion she was VP Marketing, at General Magic, where she marketed General Magic's patented voice interfaces including the voice of GM OnStar and spearheaded the market introduction of a VoiceXML voice development platform. As Director Marketing, Echelon Corporation, Ms. Skokowski led the company's product branding initiatives, creating an industry recognized standard for interoperable control networking. Earlier in her career she worked as a product manager and application programmer of high speed vision-guided robots for Adept Technology.

Ms. Skokowski has served as a Board Member of Teradata's Ecommerce Board of Advisors, Director for the ComputerWorld Smithsonian Awards Program and Executive Director to the LonMark Interoperability Association.

Ms. Skokowski received a BA and MA Honors in Engineering Science from Oxford University and an MS in Robotics from UC Berkeley.

Put Your File Transfers... Under LOCK & KEY

- SIMPLIFY
- AUTOMATE
- ENCRYPT

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

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

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by LINOMA SOFTWARE

SEE FOR YOURSELF

Find out why this grocery chain depends on **GoAnywhere™** to automate and secure daily file exchanges with vendors.

How an Aggressive Chinese IP Highlights Attribution Issues

by Tim O'Brien, Director, Security Threat Intelligence & DarkWolf Labs, Norse Corporation

Recently, the Norse DarkWolf Labs noted that the IP address 218.77.79.43 had jumped into the top quadrant for malicious activity. Investigation into the activity and the IP itself highlights the many challenges in accurately attributing such events to known actors, as illustrated in this article.

The IP - assigned to the CHINANET-HN-HY CHINANET-HN Hengyang node network, Hunan Telecom on ASN 4134 for China Telecom - had been seen targeting multiple ports and protocols over several months, and had been increasing activity in the last week of August.

From June 11, 2014 to August 26, 2014 the Norse threat intelligence platform observed over 706,000 events from this IP, with between 7,200 and 10,600 unique events each day. There had been minimal variance in the number of observed Thursdays through Mondays, and the total number for Tuesdays and Wednesdays were significantly less by comparison during that time frame.

The number of events gradually increased over the following weeks, with over 70,200 during one week alone:

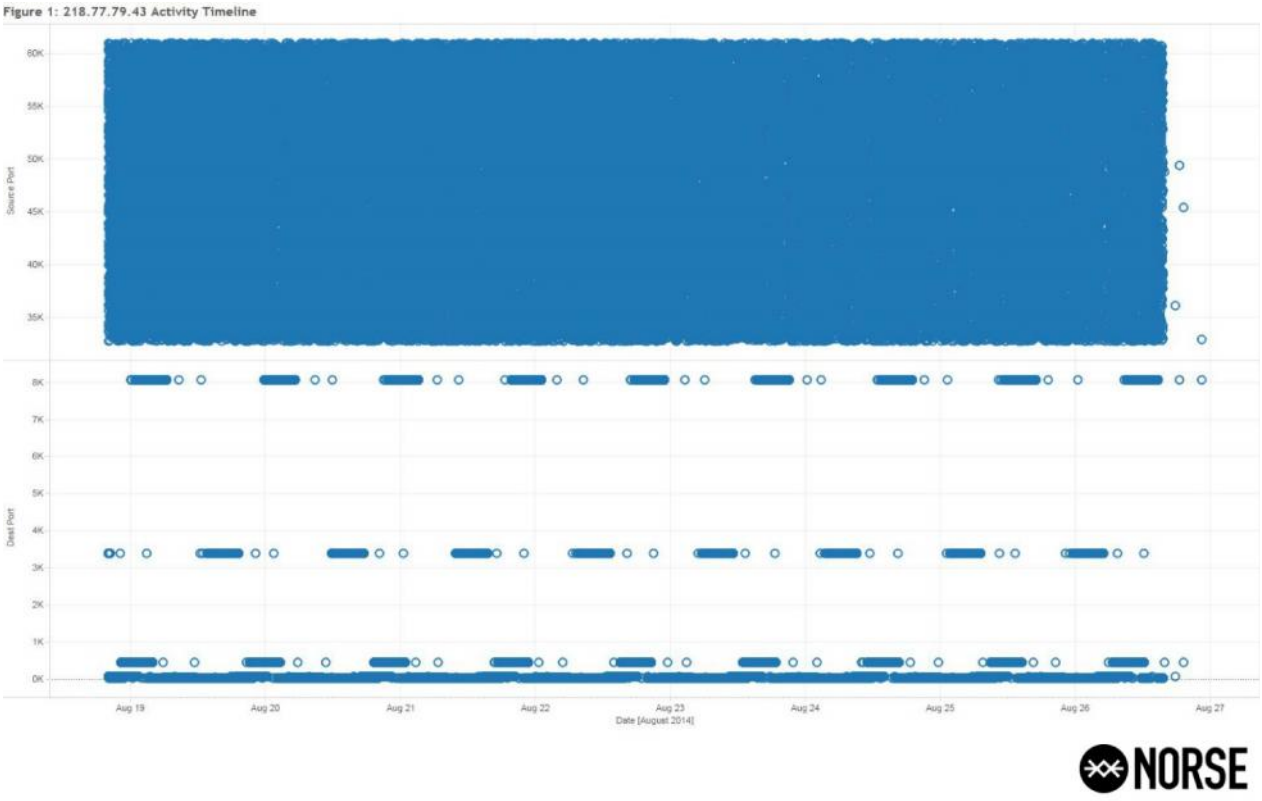


Figure One (1): 218.77.79.43 activity timeline, August 2014

The source port selection is in the 32000 to 62000 range for this activity, with the destination having a consistent pattern targeting nine distinct ports (21, 22, 23, 25, 53, 80, 443, 3389, and

8080) as displayed in Figure Two (2). Note the number of events targeting each port are relatively equivalent:

Figure 2: Destination Port Counts

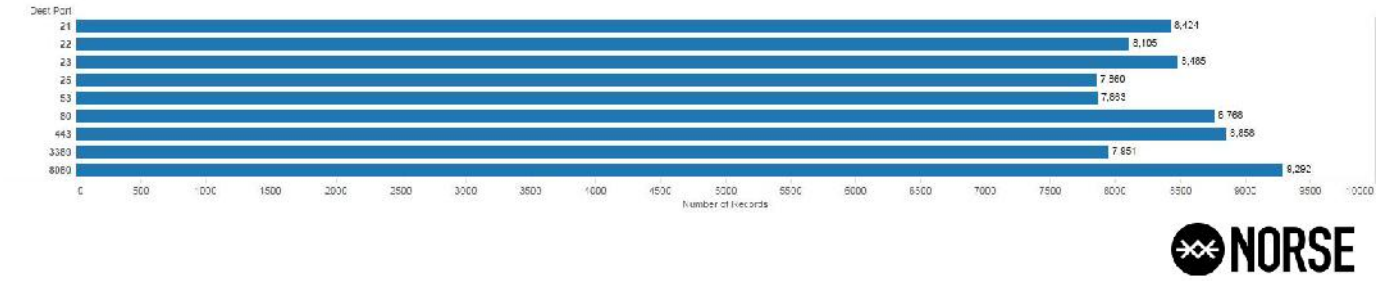


Figure Two (2): 218.77.79.43 destination port breakdown, August 2014

The activity observed indicates multiple timed and ongoing scans were occurring, with overlapping activity on the other targeted ports. The scans occurred over a six hour interval with subsequent bursts detected a few hours later.

Figure Three (3) shows a detailed view of the targeted destination ports below 1024, which display distinct patterns:

Figure 3: Destination Ports Below 1024, August 2014

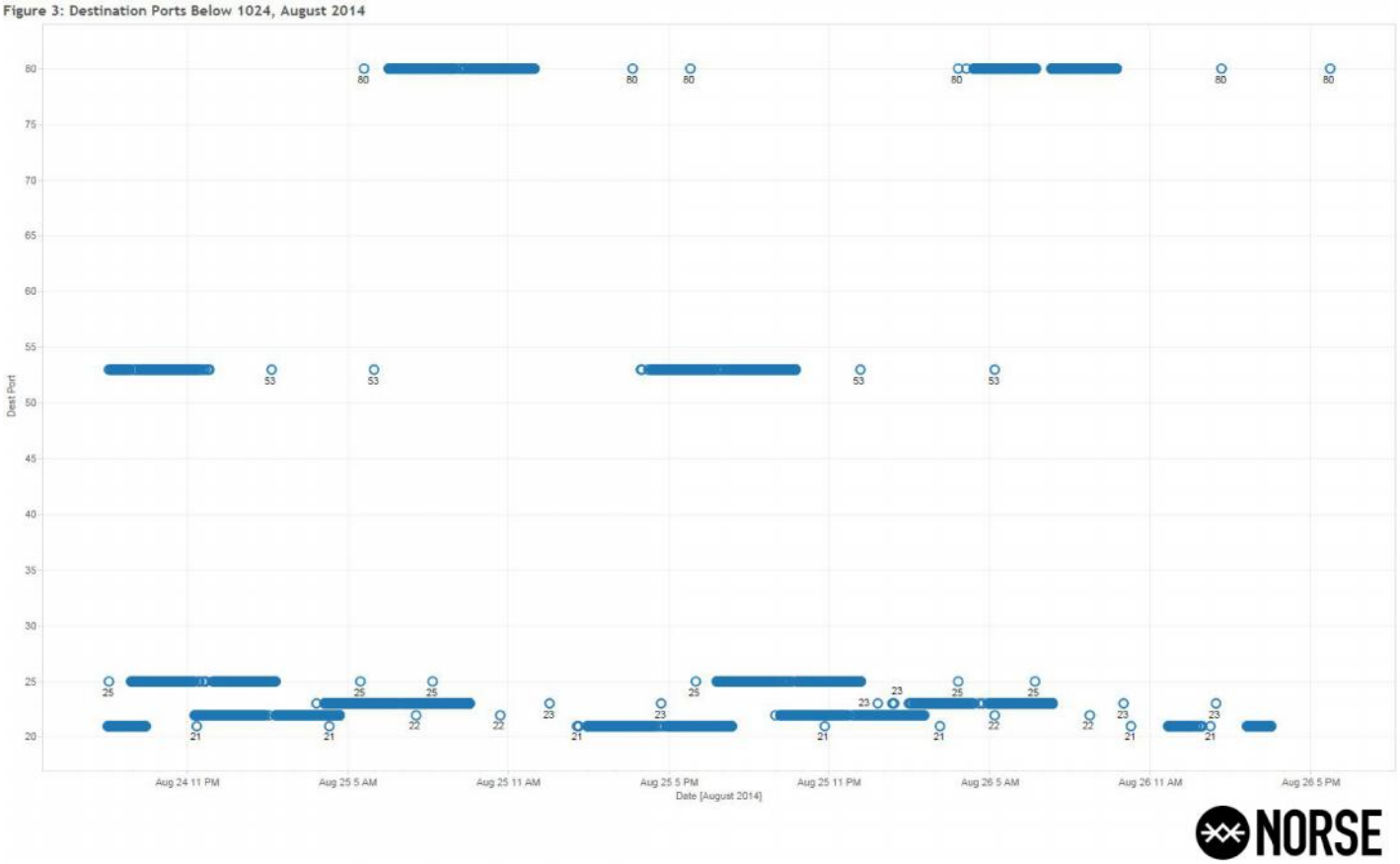


Figure Three (3): Destination Ports below 1024, August 2014

Further investigation revealed that the IP 218.77.79.43 creating this activity had been the subject of quite a bit of chatter and documentation across the Web. Researching the IP might

leave one with the impression that this was merely a Linux system with only SSH open - as was seen when it was scanned by another researcher on August 14th.This appears to be an older and not updated Linux system, considering OpenSSH 5.3 was released on October 1, 2009.

The IP in question had been submitted forty-three times to URLQuery since June 17th, 2014, with many instances showing IDS hits for being on the DShield Block Listed Source group. DShield shows similar activity starting around the same time in mid-June of 2014. The IP is also listed on ips.backscatterer.org as well as on blockedservers.com and badips.com.

This is not the first time our researchers have found a system with no public facing resources or protocols that was scanning the rest of the Internet in a systematic fashion - nor will this be the last. There are few barriers to prevent an individual or organization from setting up a system and using open source toolsets to systematically scan and attack the rest of the Internet, as long as they have an "understanding" hosting provider.

Considering the sudden increase activity has been ongoing since mid-June, it is a good assumption that the Hengyang node network of Hunan Telecom on ASN 4134 for China Telecom is being quite lenient about this customer's activities.

Following our first examination of this malicious IP, Norse DarkWolf Labs noted that 218.77.79.43 continued to hold the top spot for malicious activity, with over 66,550 events between August 26 and September 2.

Though the total events observed during this period reflected a slight decrease in observed activity from the previous week, this IP was most certainly continuing to target multiple ports and protocols, as it had been doing over the last few months.

Figure Four (4) focuses on the destination port timeline and frequency, showing the intervals of activity targeting the respective ports and protocols over this second sample period:

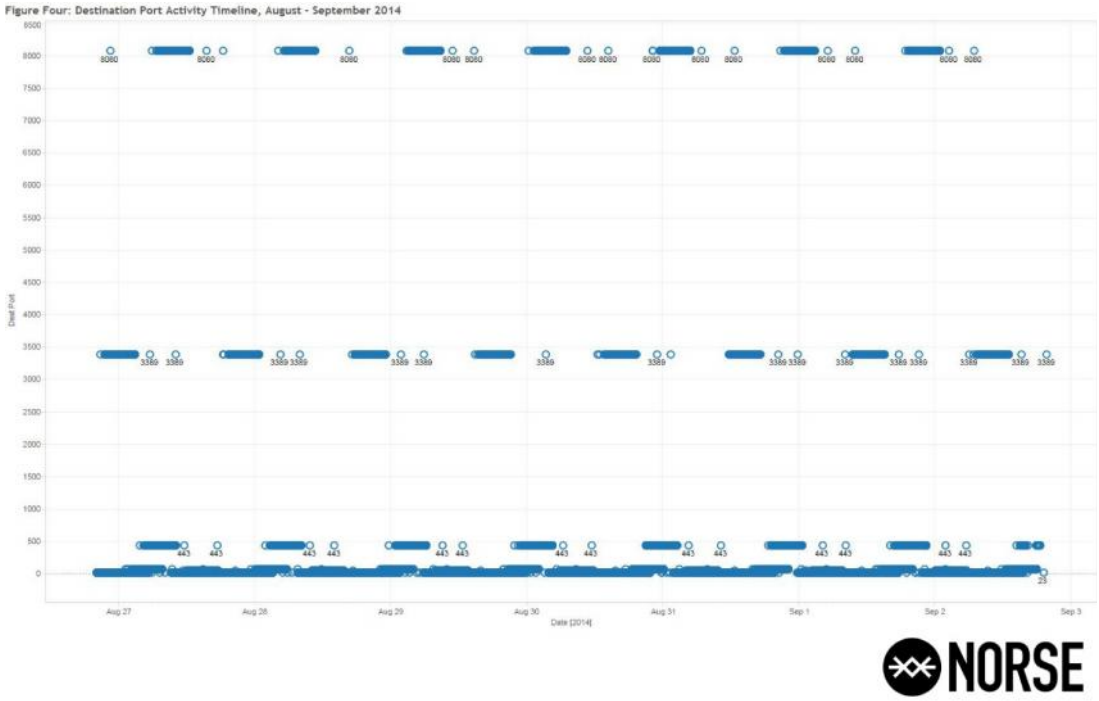


Figure Four (4): Destination Port Activity Timeline, August - September 2014.

In one of the subsequent online conversations regarding our early analysis, one security professional expressed concern regarding all traffic from this ISP, and considering CHINANET is the sole ISP for the entire country, it makes any subjective analysis quite problematic.

DarkWolf Labs found that limiting the analysis to the specific Autonomous System (AS) Number 4134 proved quite interesting, with 2,981,300 events observed from over 213,500 different IP addresses in just six months. Note that AS 4134 is not limited to Hunan Telecom or the Hunan providence, as there are hundreds of organizations and subsidiary ISPs of CHINANET using this AS Number for routing.

For comparison, Figure Five (5) breaks down the top twenty organizations for observed activity between January and August, 2014, for AS 4134. The CHINANET HUNAN PROVINCE NETWORK was clear down at number 11 in the rankings, with other providences surpassing its suspect activity:

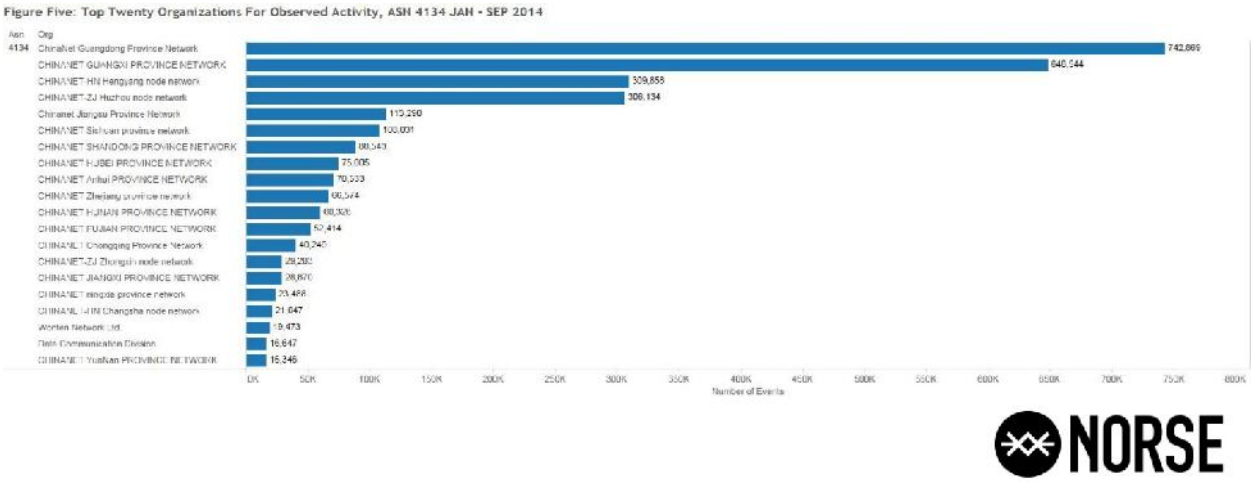


Figure Five (5): Top Twenty (20) Organizations For Observed Activity, January - August 2014.

In an effort to better understand the activity from Hunan province, Figure Six (6) plots out the locations and amount of activity detected for the province. Note the overwhelming amount of activity from around Changsha (28°10'44.4"N 113° 06'50.4"E), far surpassing any of the other observed activity for this region.

This reveals geolocation coordinates similar to those derived from the Regional Internet Registry (RIR) information for the IP address in question (218.77.79.43), and they are located either in or very near what appears to be a major waterway, the Liuyang River:

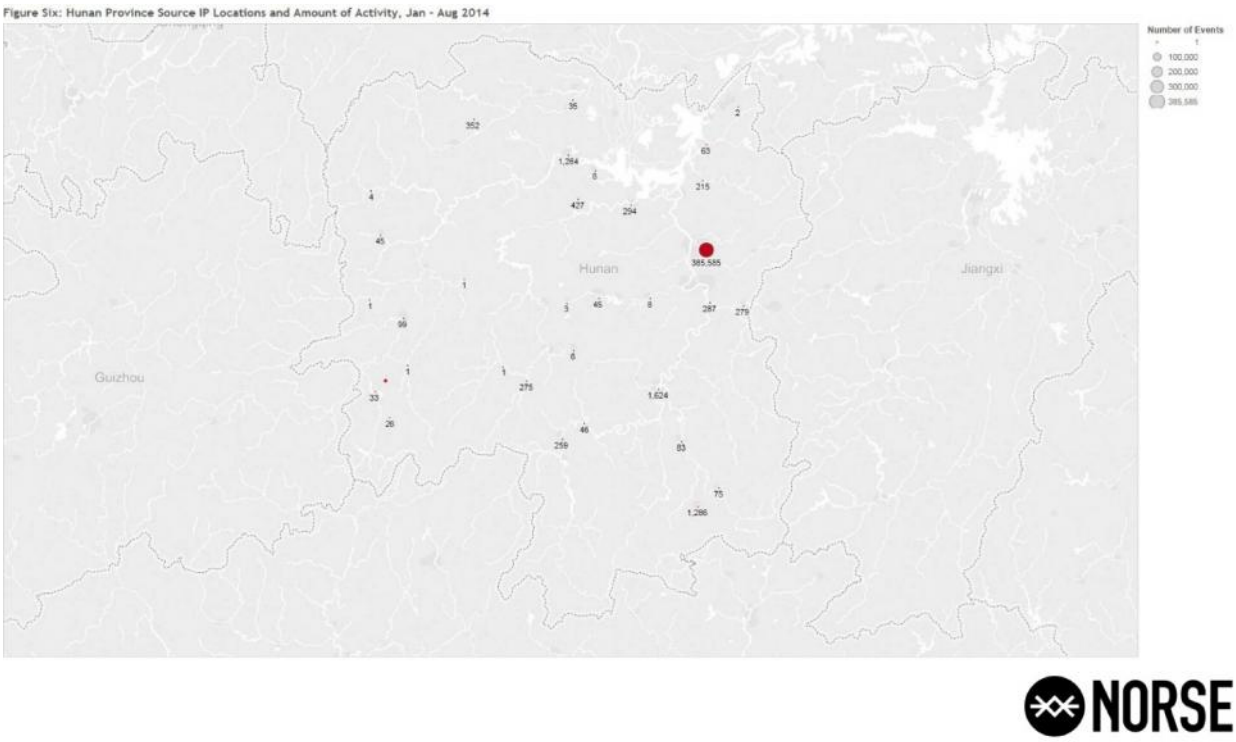


Figure Six (6): Figure Three: Hunan Province Source IP Locations and amount of Activity, Jan - Aug 2014.

In an attempt to provide attribution, by using Google Translate the DarkWolf Labs took "people's liberation army + Changsha" and obtained the Chinese translation. Searching for these terms in Google comes up with the National University of Defense Technology (NUDT), just a short distance away from the coordinates provided by the RIR:

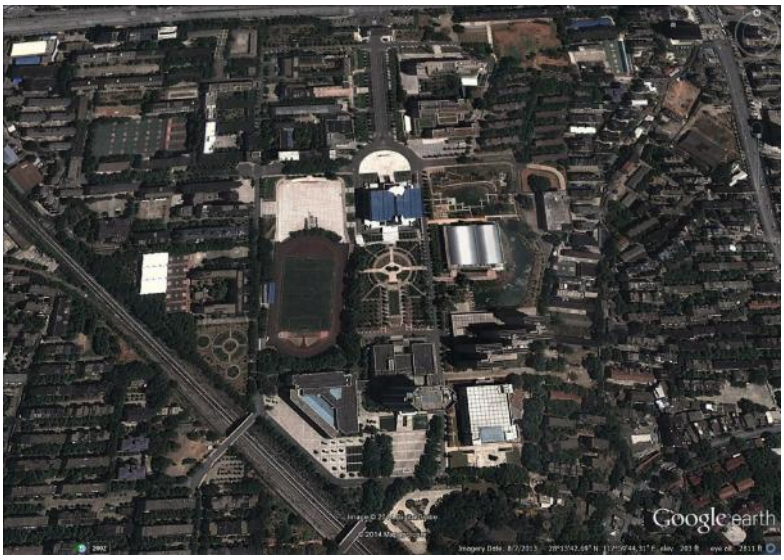


Figure Seven (7): Satellite View of National University of Defense Technology (NUDT) From Google Earth

The main entrance of the campus is at the northern most point, as depicted in the following image posted on Panoramio.com by zxpsectrum16k:

Figure Eight (8): Photo of Campus Entrance

The following week, it came as no surprise that the IP address 218.77.79.43 remained in the top aggressor list for suspect activity, with over 55,180 unique events detected between the 3rd and 8th of September, 2014.

After some more initial analysis was released, one of our readers reached out to the team inquiring as to the attribution of this IP address, sharing with us the Network Threat Blacklist System web site of the Northeastern University Network Center in Shenyang City, Liaoning Province. The System shows 218.77.79.43 as being part of Hengyang Telecom ADSL, which had been seen hitting their systems repeatedly as well.

Figure Nine (9) below shows a screenshot from the Northeastern University Network Center Network Threat Blacklist System web site enumerating the most current "top ten" threats, with 218.77.79.43 ranking at eighth:

This week's top ten threats source address

Threat source IP address	Views	Attributable
124.237.77.212	1253	Hebei Qinhuangdao City Telecom
124.237.77.247	1047	Hebei Qinhuangdao City Telecom
222.186.128.51	851	Zhenjiang City, Jiangsu Province
218.77.79.48	761	Hengyang Telecom ADSL
222.186.128.53	741	Zhenjiang City, Jiangsu Province
222.186.128.52	692	Zhenjiang City, Jiangsu Province
222.186.128.54	665	Zhenjiang City, Jiangsu Province
218.77.79.43	574	Hengyang Telecom ADSL
93.174.93.51	545	USA
218.59.238.93	522	Zaozhuang City, Shandong Province, China Unicom

Figure Nine (9): Screenshot from Northeastern University Network Center Network Threat Blacklist System web site

This raises the question as to who or what this IP address is really assigned to. The Northeastern University Network Center attributes this IP as Hengyang Telecom ADSL, but the information we receive from the Regional Internet Registry (RIR) regarding this IP is not nearly as concise.

As the screenshot in Figure Ten (10) indicates, there is no mention of Hengyang Telecom ADSL. The RIR provides the city as Changsha with a latitude and longitude nearby, and the ISP as CHINANET HUNAN PROVINCE NETWORK with the AS Name & Number as CHINANET-BACKBONE. Hengyang province is a considerable distance from Hunan province and the city of Changsha:

Network Intel	
Host	NXDOMAIN
ISP	CHINANET HUNAN PROVINCE NETWORK
Organization	CHINANET-HN Hengyang node network
AS Number	4134
AS Name	CHINANET-BACKBONE No.31,Jin-rong Street,CN

Geographic Intel	
Country	China
Region	Hunan
City	Changsha
Latitude	28.1792
Longitude	113.114

NORSE

Figure Ten (10): Screenshot from Norse DarkViking regarding IP 218.77.79.43

With the operators failing to provide truthful information regarding IP ownership and routing, the RIRs also cannot provide accurate information, and any attribution analysis can only as accurate as the information provided.

It is interesting to note that internal to China, the information seems to be more accurate than what is available from the RIRs – perhaps because it was purposefully being skewed at the RIR. Considering CHINANET is the ISP for the entire country, if ownership and routing information is not accurate or is falsified, it makes subjective analysis extremely problematic at best.

Clearly this IP is being a nuisance by scanning both internal and external hosts, and there should be concern regarding all traffic from this ISP - and potentially from this country in general - if activity of this nature continues to be tolerated.

With the activity observed from this province being just number eleven in the rankings, the members of DarkWolf Labs are curious to know what we will find in the activity from the other provinces, and will continue monitoring this activity to provide analysis and additional information to help others recognize and defend against this malicious activity.

Mitigations

From a technical perspective, having a multi-layered defense is key to detecting and stopping malicious activity early, which also helps with overall detection rates, thus minimizing the impact to an organization when defenses fail.

A good methodology to start with for any organization would be the Council on CyberSecurity's 20 Critical Security Controls, which are geared towards addressing the key threats confronting networks today, as they are continuously being reviewed and updated.

An additional measure in your multi-layered defense is ensuring network and system monitoring and detection is in place through your IDS/IPS, with the alerts being fed into your log management/SIEM solution for review, analysis, and potential action.

Furthermore, organizations can take proactive action regarding suspect actors conducting scanning/reconnaissance of your infrastructure by using host based tools such as DenyHosts, FailToBan, or a Windows platform equivalent.

A more robust, supportable solution and force multiplier would be leveraging a robust threat intelligence (TI) platform, enabling you to block these miscreants and associated activity at your network boundaries, and clearly identify them in your log management/SIEM solution for review, analysis, and potential action according to your specific security policies and acceptable level of risk.

About The Author

Tim O'Brien is Director of Security Threat Intelligence & DarkWolf Labs at Norse Corporation. As a 15-year information security professional, O'Brien is a subject matter expert in risk and incident management, intrusion and data analysis, secure architecture design, and systems management. O'Brien is well versed in developing technical solutions, determining the best options for the business and its goals, and creating comprehensive implementation plans that minimize risk for the organization. His excellent analytical and problem solving skills, with emphasis on understanding relationships among technical problems, result in sound and effective business solutions while reducing risk. He enjoys mentoring others and helping them develop their skills through supervisory positions, coursework development, mentoring, presenting at and helping run information security conferences, as well as instructional positions. Tim can be reached online at to@norse-corp.com or at his company website http://www.norse-corp.com/.

2014 SMART CYBER DEFENSE

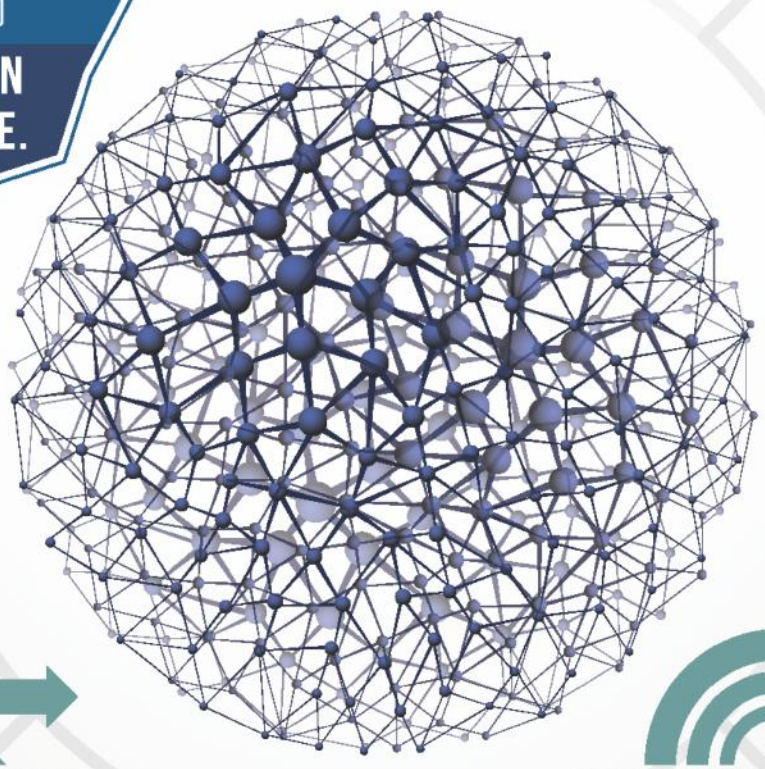
CAXTON TECHNICAL TRAINING COURSE

23 - 27 NOVEMBER 2014 | ABU DHABI. UAE

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

SAVE 10% ON TRAINING FEE.

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



SMART CYBER DEFENSE COURSE 1:
SOLID DEFENSE STRATEGIES

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

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

www.caxtongroup.com

The Top Ten Mobile Flashlight Applications Are Spying On You. Did You Know?

SnoopWall CEO, Gary Miliefsky, a Founding Member of Department of Homeland Security, Recommends that Everyone with a Mobile Device Should Immediately Delete their Mobile Flashlight Apps

by Gary S. Miliefsky, CEO, SnoopWall - Privacy & Security Expert

October, 2014 marks the beginning of the 11th annual National Cyber Security Awareness Month (see: http://staysafeonline.org/ncsam/). What better time than now to realize you are being spied on. Why does Brightest Flashlight need to Geolocate you? It doesn't. For that and other privacy reasons, that's why the FTC recently sued them. However, the FTC was mostly concerned with their privacy policy. ***Do you even read the privacy policy of the apps you install?*** Most people don't. Here's the story: http://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app

Everyone wants a flashlight app on their phone. Finding your keys, searching for something you lost, looking for the light switch in a hotel room? What a great utility, right? Wrong! The top 10 free flashlight apps in the Google Play store alone account for nearly 1/2 BILLION INSTALLATIONS are all spying on users with an application size ranging from of 1.2 to 5 megabytes. In fact, an optimized flashlight application should only be 72k which is 10-50 times smaller than the smallest one of these apps. So, why so big? The size is significant because there's a lot more code than necessary embedded in these applications which allows them to eavesdrop on you. Nothing in life is free. These flashlight apps do some very strange things – geolocate you, read your contacts list, read your device storage looking for personal, sensitive pictures and videos, read and write files, check to see what apps are running, look for ways to communicate over the internet (wifi or cellular), get your phone number and so much more that SnoopWall considers all of them well designed MALWARE. All of them!!!

It's obvious to us at SnoopWall that these applications are designed to expose your personal information to cybercriminals or other nation states (such as China and Russia). In addition, you are at significant risk if you are doing Mobile Banking on the same device as one of these free Flashlight Apps. Our strong recommendation is to uninstall your flashlight app immediately.

For a full copy of SnoopWall's Flashlight Apps Threat Report, visit http://www.snoopwall.com/threat-reports-09-29-2014/

While the FTC.gov has gone after one of these ten vendors, it seems they are still at it and the other 9, as well. It seems time to ask "where's the outrage?" - shouldn't you UNINSTALL your FLASHLIGHT APP today? The answer is yes! You might also want to contact the FTC and tell them you are concerned.

We've come up with a list of what we think are best practices for increasing privacy and security on your device without spending any money. This is based on SnoopWall's counterveillance research for improving your privacy from eavesdroppers and helping you from getting infected with spyware that could cost you your identity. They are:

1) Disable your GPS at all time except in an emergency or when you need to use your smartphone for navigation purposes;
2) Disable your NFC (Near Field Communications) or on Apple devices, iBeacon, permanently (http://support.apple.com/kb/HT6048);
3) Disable Bluetooth at all times except when you are in your car, driving, if you want to have hands-free calls, if supported by your car;
4) Verify Apps behavior and privacy risk BEFORE installing – do some research and ask the questions "why does this app need GPS, MICROPHONE, WEBCAM, CONTACTS, etc.?" – most apps don't need these ports unless they want to invade your privacy. Find an alternative before installing risky Apps;
5) Either put masking tape over your webcam and microphone when not in use or pull the battery out of your smartphone when you are not using it.

Obviously for #1, there's no need for geolocating you, unless you don't mind being spied upon by these malicious flashlight apps – or worse – your children's location being monitored by online predators. Best to keep this hardware port disabled until you really need it.

For #2, you're probably wondering "what the heck is NFC and why should I care?". We'll it's a new protocol for 'bumping' or getting close to other devices, within 3 meters or so, to exchange information such as photos and contacts. Is it secure? No. Can it be hacked just like Bluetooth? Yes. Go into your device settings, find NFC, if you see it, disable it.

Ok, for #3, you're thinking 'that makes sense' – Bluetooth is an easily hacked protocol and folks can eavesdrop on communications over Bluetooth; broadcast into your earpiece (yes, it's been done); access your contacts list and hack your smartphone device over Bluetooth. So, if you disable this protocol everywhere except when you are in the car, wanting a hands free experience for making and receiving calls, you should be much more secure.

For #4, how many times do you install an app with excitement about promised features and functions, only to find that it requires incredible privacy risk? If it's too good to be true it probably is and nothing in this world is free. There are 9 major advertisement networks and some deploy spyware. Free apps use these networks to monetize their businesses and some are developed by professional cyber criminals, enemy nation states for spying or by hackers for malicious reasons.

We really don't like making recommendation #5 but until you try out our SnoopWall product, there's really nothing you can do to block webcam and microphone eavesdropping, so why not make it hard for the bad guys to see or hear anything useful?

Because some of the Flashlight Apps write settings and have access to your device storage, it may be to install additional backdoors or remote access Trojans (RATs), therefore you might need to reset your phone completely after an uninstall of your favorite Flashlight App. Some might even wish to go to FACTORY RESET or a WIPE. Once you've cleaned off the Flashlight RAT, you might still want a flashlight app on your phone that you can trust.

WARNING: Don't reset or wipe without backing up ONLY those contacts and files you are certain to trust. If you do a complete device backup and restore, you risk also restoring malware. Ask a friend who is an expert with your kind of phone or the staff at the store you purchased your smartphone or tablet on how to do this the right way.

We developed the **SnoopWall Privacy Flashlight** for Google Android, Apple iOS and Microsoft Windows smartphones and tablets. The file size of the SnoopWall Privacy Flashlight application is approximately 72 kilobytes. It only accesses the light of the webcam and the screen display which is all a flashlight app should be doing anyway. Get it today at: http://privacyflashlight.snoopwall.com

We've also developed another free application called Privacy App which will scan your Android or Windows device and show you which apps are spying on you. If you have suspicions, confirm them with Privacy App. Learn more about our technology and products at: http://www.snoopwall.com/products/

About The Author

Gary S. Miliefsky is a Counterveillance expert and founding member of the U.S. Department of Homeland Security, Gary Miliefsky, is the Founder of SnoopWall and the sole inventor of the company's technologies. He has successfully advised two White House administrations on cyber security, filed more than a dozen patents of his network security inventions, and licensed technology to major public companies, including IBM, BlackBox Corp. and Computer Associates International. Gary is a recent Editor of Cyber Defense Magazine. He also founded NetClarity, Inc., an internal intrusion defense company, based on a patented technology he invented. He also advised the National Infrastructure Advisory Council (NIAC) at the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. Miliefsky serves on MITRE's advisory board and its CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (www.NAISG.org). 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. Gary is a prolific author, a frequent presenter and subject matter expert on topics related to digital privacy, counterveillance and cybersecurity for corporations and the news media.

SOURCE SnoopWall

10 Architectural Principles that Prevent Code Modification or Reverse-Engineering

by Jonathan Carter, Technical Director, ***Arxan Technologies***

When trying to prevent reverse-engineering or unauthorized code modification into your mobile app solution, there are ten critical design principles that should be applied to your solution. Together, these architectural features will make it very difficult, if not impossible, for an attacker to inject or modify mobile app code through binary attacks.

#1 Principle to Follow: Defense in Depth

Integrity controls within applications must be applied using a defense-in-depth strategy within the application binary. A network of integrity controls should protect each other as well as the underlying application. This integrity control layering strategy makes integrity vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur.

For example, checksum controls should protect other checksum controls that verify the integrity of the application. This makes it a tedious and difficult task for an attacker to tamper with the integrity verification mechanism.

2. Positive Security Model

A "positive" integrity security model applies code integrity controls to protect code and data based on characteristics that are known and good, rather than what is known to be bad. This reduces the amount of maintenance involved in maintaining integrity controls within the application over time.

For example, a value-verification integrity control should verify that a data element holds particular values when it needs to verify that the application has not been tampered with. It should not look for known bad values as these values may grow over time with new, unknown avenues of attack.

3. Avoid Integrity Information Leakage

Handling errors securely is a key aspect of application integrity protection. When integrity controls detect tampering, the organization may want the application to fail. The application must do so without revealing information about the underlying technologies that implement the integrity controls.

For example, it would not be appropriate for an integrity control to respond to an attack by displaying an error message that indicates the specific integrity control that failed.

4. Least Privilege

Applications must run under accounts that have the least amount of privilege required to perform their business processes. When code integrity violations occur, the control should not require elevated privileges to respond.

For example, an integrity control should not respond to an attack by executing sensitive functionality exposed through an administrative API service.

5. Avoid Integrity Security by Obscurity Alone

Security through obscurity is a weak security control, and nearly always fails when it is the only control. The security of key systems should not be solely reliant upon keeping details hidden.

For example, an application should not solely rely upon an obfuscation control to prevent an attacker from understanding the application. In addition to obfuscation, the application could include Static Damage, Checksum, and the many other types of code integrity controls working together.

6. Simplicity

Attack surface area and simplicity go hand in hand. Architects should avoid the use of integrity control architectures if it is possible, and does not adversely impact business models, to eliminate the storage or processing of sensitive assets in untrustworthy environments.

7. Detect Integrity Violation Incidents

Detecting code integrity violation incidents are important because otherwise the attacker has unlimited time to perfect an integrity attack. An integrity violation is defined as an insertion of code into the application.

For example, a Checksum control is responsible for detecting code changes between compile-time and runtime of the application.

8. Don't Trust Infrastructure

The operating environment of an application must never be trusted. Although an application may be deemed secure in one environment, it may eventually be used in an unforeseen way in an unforeseen environment.

For example, web application code may be reused within mobile application code. In such a scenario, the web application's business layer code may be hosted in a more controlled (trustworthy) environment while the same web code is later moved into a less controlled (untrustworthy) mobile environment.

9. Establish Secure Defaults

There are many ways to deliver an "out-of-the-box" experience for users. However, by default, the experience must be secure. By default, the application should have integrity controls turned on.

For example, it is advisable to force application integrity controls to be automatic and on at all times within the mobile application. Such controls should not be active based on an external configuration file. If this dependency existed, it would be possible to accidentally release an application with an inactive integrity control.

10. Don't Trust Local Resources

Many organizations leverage third-party libraries and other external file-based resources. Where possible, application controls should verify the integrity of these external dependencies as well.

For example, a mobile device application may rely upon JavaScript that is executed in a local browser. The application should verify the integrity of this external resource before loading it into a browser on the device.

Parting Thoughts

Mobile app developers must now take into account a whole host of new risks that relate to hosting code in an uncontrolled environment. If you are hosting code in an untrustworthy environment, you are susceptible to these risks.

As such, a holistic approach is needed that can detect, react, and alert to unauthorized code modifications or reverse-engineering within the mobile app. With such an approach, hackers are kept further at bay, and the odds of a network breach significantly drop with sensitive data that is more difficult to decipher.

About the Author

Jonathan Carter is the technical director of Arxan Technologies. He has over 15 years of security expertise within Canada, United States, Australia, and England. Jonathan has produced software for online gaming systems, payment gateways, SMS messaging gateways, and other solutions requiring a high degree of application security.

Jonathan's technical background in artificial intelligence and static code analysis has lead him to a diverse number of security roles: Enterprise Security Architect, Web Application Penetration Tester, Fortify Security Researcher, and Security Governance lead. Jonathan can be reached at (301) 968-4290 and at our company website http://www.arxan.com

Using Automated Threat Response to Mitigate Security Events

by Paul Nguyen, President of Global Security Solutions at CSG Invotas

There's a big story in cybersecurity today, but no one's covering it. Sure, data breaches are attention-grabbing, headline-making events—and let's face it, there have been plenty around to choose from. And yet it's not the shock of discovering a breach or the high-profile identity of many of the recent targets but the inevitability of a breach occurring that the headlines ignore. The question has shifted from, "Will I be attacked?" to, "When the attack happens, will I be prepared?"

We know that attacks routinely target critical networks and that they are as likely to affect multiple organizations in a single or related industry as they are to focus on one target. What's surprising is the length of time it takes organizations to detect and resolve those attacks. Security events can unfold in the blink of an eye but can take months—even years—to be properly identified and eradicated from an organization's systems. Recently released IDG survey results show that while more than one-third of cyber attacks take hours to detect (which is relatively fast in today's climate), resolving breaches takes days, weeks and, in some cases, even months.

Situational Analysis

We need a seismic shift in the ways we respond to, mitigate, and remediate threats. To support holistic cyber risk management, organizations must deploy adaptive technologies that transform dynamically in real-time to foil cyber attacks. Instead of simply detecting and analyzing incursions, neither of which triggers an actual response to or containment of an attack, organizations can adopt strategies that include automated threat response and real-time security orchestration solutions. Such solutions can be configured to act on business- and security-event triggers to initiate successive and adaptive actions across an enterprise to reduce potential damage. Attacks that come in looking like one piece of software code quickly mutate and adapt to the target environment, multiplying the number and types of attacks and proliferating at machine speed to expose weaknesses. New cyber threats are growing in the ability to act autonomously with behavior that is customized to a specific target; they utilize multipart designs with self-concealing, mutating, and hibernating capabilities.

To combat these sophisticated attacks, continuous monitoring architectures can provide real-time situational awareness of threats and vulnerabilities but fall short of providing the ability to make machine-speed risk management decisions, mitigations, and responses to successfully defend and respond to security incidents. The ability to enable a quick response to a breach should be the focus of C-suites everywhere, but without the ability to take near real-time action, what is the point? We don't need to continue to focus our resources solely on detection. We don't need another set of watchful eyes. We already have far too many eyes, and they're still not seeing the threats. Automated threat response enables the command and control of continuous monitoring architectures to dynamically adapt and respond to security incidents or emerging threats in real-time—the next sea change in cybersecurity defense.

The Road Forward

Business as usual is no longer good business where cybersecurity is concerned. Continuous monitoring and other defense efforts are a good first step, but they need to be taken further. We know the gap between detection and response grows wider every day, and we know the speed, versatility, and frequency of attacks have reduced the effectiveness of traditional threat responses. Today's cyber defenders require the ability to correlate, act, defend, and mitigate in near–real time to prevent the proliferation of cyber attacks enabled by workflow and remediation.

We need speed. We need smarts. We need the power and control to change networks on the fly. We need to respond in minutes or seconds to stop intruders in their tracks. We need to close attack windows within seconds to reduce the risk to critical infrastructure. We need to stop following rules that our attackers openly flout. And finally, we need to shift networks dynamically to spoof attackers and allow our defensive tactics to appear as random to malicious actors as their attacks so frequently appear to us.

Automated threat response enables the implementation of pre-determined defensive strategies at machine-speed for the isolation, regeneration, or redirection of malware and other malicious threats. Pre-planned risk-mitigation strategies that can be implemented in near real-time across servers that contain invalid information, or files that contain payloads or beacons in expected exfiltration files as an attack is occurring, enables organizations to curb attacks without human intervention, thereby reducing the exposure window.

Automated threat response accomplishes these types of tasks by seamlessly integrating heterogeneous security solutions (firewalls, intrusion detection systems, Web applications, mobile device management, and the like) using security orchestration as the mortar that binds solutions together in a cohesive, holistic - defense architecture. Security orchestration acts as a multiplier for risk mitigation by implementing actions across the network without having to coordinate actions manually.

Security orchestration means security administrators and analysts don't have to distribute threat information to other administrators and analysts in order to act. And that means security teams no longer have to be held hostage by outmoded processes, hampered by red-tape, bound by strict adherence to rules, or hindered by varying levels of competence, all of which stall effective and efficient response orchestration.

CISOs agree. IDG research shows that 61% of security decision makers surveyed are looking into ways to reduce the time it takes to respond to a security event. A quarter of those surveyed said they are in favor of automating some security processes and use automation tools where possible.

In cybersecurity, the offense generally has the advantage. But defense need not be passive; superior maneuverability offers a powerful alternative to traditional defensive strategies. Instead of responding to every attack equally, we can orchestrate the workflows that coordinate tools to work together to support comprehensive—but unpredictable—defensive plays that can be generated at the speed of attack. We can integrate automated tasks to replicate decisions faster– that in turn change attack targets and confuse attackers' perceptions. Coordinated responses coupled with active defense can provide the necessary flexibility and adaptability to keep security assets online and secure.

About the Author

Paul Nguyen, President, CSG Invotas Global Security Solutions

Paul specializes in governance, risk, compliance solutions, information management, and information security strategy for global communications and systems integration organizations that have included KCG, Neohapsis, Deloitte, Symantec, BearingPoint, and Telcordia. He is a well-known cybersecurity expert and frequent contributor to media outlets such as CSPAN, ISC2, WashingtonExec, Government Executive, Federal Computer Week, and Government Computer News. He has published numerous articles, white papers, and security assessments to the federal government and commercial clients.

Your Server as the Last Line of Cyber Defense

By Scott Schweitzer, Sales Manager OEM & Federal Southeast, Solarflare

Since the days of medieval castle design, architects have cleverly engineered concentric defensive layers along with traps, to thwart attackers, and protect the strong hold. Today many people still believe that the moat was a water obstacle designed to protect the outer wall, when in fact it was often inside the outer wall and structured as a reservoir to flood any attempt at tunneling in. Much like these kingdoms of old, today companies are leveraging similar design strategies to protect themselves from Internet attackers.

The last line of defense is always the structure of the wall, and guards of the castle keep itself. Today the keep is your network server that provides customers with web content, partners with business data, and employee's remote access. All traffic that enters your servers comes in through a network interface card (NIC). The NIC represents both the wall, and the guards for the castle keep. Your NIC should support a stateless packet filtering firewall application that is authorized to drop all unacceptable packets. By operating within both the NIC, and the kernel driver, this software application can drop packets from know Internet marauders, rate limit all inbound traffic, filter off SYN floods, and only pass traffic on acceptable ports. By applying all these techniques your server can be far more available for your customers, partners, and employees.

Stateless Packet Filtering Firewall on the NIC & Address Based Filtering

Filtering off traffic from known bad actors on the Internet requires two things: a current list of the malicious IP address (or address ranges) and a filter engine capable of apply this list to all inbound traffic coming through the NIC. Several companies provide up-to-date address based lists of known cyber terrorists. For example Norse has a product called the Norse Darklist™ that is an enormous collection of confirmed high-risk IP addresses, which is continuously updated. Every address on the list has a threat score, a country of origin, threat category, and the date it was last detected. Here is a snippet of what this list looks like:

Action	IP	IPQ_SCORE	LAT	LONG	COUNTRY	CATEGORY	PROTOCOL	LAST_SEEN
+	2.0.343.152	97.1	7.909	98.3332	TH	Botnet	Bot	11/12/2013 3:24
+	31.131.30.210	94.7	33.7257	-84.4309	US	Proxy	IP based proxy	11/19/2013 1:34
+	46.38.7.58	90.7	48.4808	135.093	RU	Bogon Unadv	IP Unadvertised	11/15/2013 1:31
+	50.22.130.187	100	32.9299	-96.8353	US	Proxy	Web Proxy	11/19/2013 8:56
+	54.213.1.27	100	40.5525	-74.2915	US	Passive DNS	Malware domain	11/11/2013 2:15
+	79.19.216.131	99.3	41.9	12.4833	IT	Proxy	Tor Exit	11/17/2013 1:13
+	124.228.42.141	94.2	26.8881	112.615	CN	Malware	Malware URL	11/18/2013 3:02

One could subscribe to this list, then cull it down to only those addresses above a certain score, and seen in the past six months. The resultant list could then be loaded into a NIC with stateless packet filtering firewall technology like those offered by Solarflare in their Flareon series of adapters. With one of these NICs running SolarSecure™, Solarflare's stateless firewall technology, all traffic from these high-risk IP addresses would be dropped. Both the

filter, and a very brief list structured to work with SolarSecure™ might look something like this; note execution starts at “start_src_filter”:

```
set_max_channels 2
set_default_action accept
set_max_objects 5
set_max_miniaddrs 5
ip4tbl_alloc high_risk linear 3 none

start_code
        accept:
                load 1 r0
                stop
        reject:
                load 0 r0
                stop
        start_src_filter:
                test_ip4
                jmp_if_not accept
                append_ip4_src pkey
                lookup high_risk p1
                stop
end_code

ip4tbl_insert high_risk 160.1.1.0/24    reject
ip4tbl_insert high_risk 2.0.334.152/1   reject
ip4tbl_insert high_risk 31.131.30.210/1 reject
```

To use this filter you would simply start the filter engine and tell it where to enter the configuration file. Suppose we saved the above text in a file called “example.conf” then the command used to start SolarSecure™, and load the configuration file would be:

```
solsec_fe –I eth2 go example.conf start_src_filter
```

Rate Limiting Inbound Traffic

Next we should rate limit or throttle back incoming packets by IP address. This keeps traffic flowing, but allows you to retain a handle on any attackers. In our example we permit 1,000 packets per second by restricting packet flow to 10 packets every 10 milliseconds from any given address. If someone were uploading a file to your server this would establish roughly a 12Mbps bandwidth limit (1,000 packets of 1,500 bytes each per second), which is typically ten times faster than the average US residential upload speed. If this were in-fact an attacker from a well-connected cloud provider it would restrict them to the same 1,000 packets per second instead of potentially tens of millions of packets per second. Since most of these attacks utilize small packets even the most powerful attacker would only consume typically 500Kbps of bandwidth or 1/20,000 of your link bandwidth, versus all of it. This could mean the difference between your server experiencing a minor annoyance versus being shutdown. Here is an example of a rate-limiting filter (sans header), note the entry point is “rate_limit_1kpps”:

```
start_code
        accept:
                load 1 r0
                stop
        reject:
                load 0 r0
                stop
        rate_limit_1kpps:
                channel_state p1 u64 -
                test_rate_le p1 0 10pkts 10ms
                jmp_if_not reject
                jmp_accept
                stop
end_code
```

Defending Against a SYN flood

A SYN flood is one of the most common Denial of Service (DoS) attacks. SYN floods made up well over 30% of the DoS traffic over the past year, and it's use is growing. Recently a large web retailer was found to have had part of its cloud service compromised, and redirected as a DoS attack platform. Fortunately for packet filtering NICs this type of assault is fairly easy to deal with. Very few attackers respond to the ACK your server would normally generate in response to their SYN request. If we move the creation of this ACK from the operating system to the NIC we can free up the OS, and host CPU, thereby removing the resulting impact of this attack on your server. Coupled with rate limiting incoming traffic, any SYN flood that would make it to your server would no longer significantly impact it. Here is an example of a SYN filter, sans header, that could be added to address a SYN flood assault, note the entry point is "start_filter_syn":

```
start_code
        accept:
                load 1 r0
                stop
        reject:
                load 0 r0
                stop
        start_filter_syn:
                test_ip4
                jmp_if_not accept
                load_tcp_flags r2
                test_mask_match r2 syn syn
                jmp_if_not accept
                jmp reject
                stop
end_code
```

Filtering by UDP & TCP Port

To stop accesses to all UDP & TCP ports, except those we find acceptable, one would simply craft another filter. The easiest way would be to first reject all port requests, then

accept all requests for what this server should doing. Here is an example of how this might be done for a web server that should ONLY be responding to port 80 requests on the production interface:

```
set_max_channels 2
set_default_action reject
set_max_objects 5
set_max_miniaddrs 5

start_code
        accept:
                load 1 r0
                stop
        reject:
                load 0 r0
                stop
        start_only_http:
                test_ip4
                jmp_if_not reject
                test_tcp4 first_frag
                jmp_if_not accept
                load_ip4_dport r2
                test_eq r2 80
                jmp_if accept
                load_ip4_sport r2
                test_eq r2 80
                jmp_if accept
                jmp reject
                stop
end_code
```

Creating a Multi-stage Filter Pipeline

In many cloud environments, data center managers need to separate and isolate traffic at each virtualized server. They need more flexibility than that allowed by the dedicated firewalls at the periphery of the network, the access control lists available on the network switches, or other expensive dedicated security appliances. Solarflare currently has customers using the SolarSecure™ Filter Engine in VMware environments. The above examples work just as well in VMware ESXi multi-tenant cloud environments that need to separate and isolate traffic by service type and customer. Customers can now implement these security functions natively in the host, and make security decisions lower in the stack offloading the host for greater performance, efficiency and enhanced security. Recently a large cloud provider using 10GbE

adapters purchased from a commodity supplier, saw an 80% increase in throughput as a result of switching to Solarflare's high performance Flareon adapters running SolarSecure™.

Much like the medieval castles of the past with layered defenses, multiple filter engines can be created, each with a different configuration file, resulting in a multi-stage filter to protect your server. Each stage can then be updated on-the-fly loading new configuration files as new Internet marauders pop up, or you business need changes. So using all the above examples in concert your server could defend itself from attacks originating from high-risk addresses, rate limiting all remaining traffic to 1,000 packets per second, screening off any SYN flood traffic that makes it past your perimeter, and finally dropping all port requests except those for port 80. This demonstrates both the power, and flexibility of the filter engine technology. All of the above samples are variations of those presented in the SolarSecure™ User's Guide. This further demonstrates the ease of use of the filter engine with regard to creating new filters.

About The Author

Scott Schweitzer is the Sales Manager of OEM, Federal, and Southeast for Solarflare. He is technology entrepreneur with a strong background in both hardware & software, combined with a unique talent for solution-based sales. Scott joined Solarflare in August 2013 to manage the relationship with IBM – while driving 10 & 40GbE sales into the federal sector, and the southeast. Prior to that he spent eight years leading Myricom's 10-Gigabit Ethernet sales team.

Scott can be reached online at (sschweitzer@solarflare.com, @40gbe) and at our company website http://www.solarflare.com/

WHAT TO EXPECT

EXHIBITION SPACE

27,000 SQM

EXPECTED NUMBER OF EXHIBITING COMPANIES

250

EXPECTED NUMBER OF TRADE VISITORS

8,000

450
KEY DECISION-MAKERS FROM INTERPOL'S

190
MEMBER COUNTRIES

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

Event Owner: INTERPOL

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

Supporting Knowledge Partner: Frost & Sullivan

Held In: YourSingapore

Managed By: MP international

The CISOs struggle for respect in the enterprise

Within the past year, the role of Chief Information Security Officer (CISO) has become increasingly visible in the enterprise. The position has evolved from a high-level IT administrator into a C-level executive, one who has been under constant pressure. The cause for the heightened visibility is unfortunately all too easy to identify – since the Target breach, media coverage of data breaches has intensified, bringing cybersecurity into the public eye. Not a week goes by without a high-profile breach in the headlines, and it is creating speculation in the press and beyond about what enterprises and governments are doing to fight cybercrime.

In the past year, boards have appointed CISOs as a way to quell cybersecurity fears. But, these newly minted members of the C-Suite have not been properly empowered, oftentimes given limited decision-making authority and no power over the purse strings. Recently, we partnered with Opinion Matters to conduct a survey of 203 C-level executives across the country in a variety of vertical markets to better understand how they view the role of the CISO. The results demonstrated that the rest of the executive team believes that CISOs should be held at arm's length, with 74 percent responding that CISOs did not deserve a seat at the table and should not be part of an organization's leadership team. Additionally, 44 percent of C-level executives said that CISOs "should be accountable for any organizational data breaches," essentially serving as a scapegoat should a breach occur. Surprisingly, just 27 percent actually believe their CISO contributes greatly to improving day-to-day security.

The overall response to the survey indicates that CISOs are held in little regard by their peers. But, the survey also shows that in many cases, CISOs have not been put into position to succeed. Without the power to make strategic or spending decisions, CISOs are unable to make an impact on cybersecurity within their organizations. There is also confusion as to whom the CISO should report to, with different organizational structures placing them under the CEO, CIO, or even CFO. With the role of the CISO so undefined, it is easy to see why many executives are skeptical – they likely do not understand what the CISO is there to accomplish.

When CISOs are given the proper authority, they still have to manage a delicate relationship between cybersecurity policy and the needs of the business. Leadership realizes that in the age of data breaches they can no longer afford to pay lip service to security issues. But, if good cybersecurity practice were to get in the way of a business function, it is doubtful that CISOs would be able to convince their C-Suite peers to take action. Further, it is unclear whether enterprises are willing to do whatever it takes to protect their data – or their customer's – if it has an effect on the bottom line.

The CISOs seat at the table won't be earned easily; it will be hard fought, with change needing to come on both sides. One of the first steps CISOs can take to rectify this problem is to become more involved in business functions, and to gain a better understanding of business objectives and goals. More than two-thirds of executives surveyed thought that CISOs didn't possess awareness of organizational goals beyond cybersecurity, and that may explain why they are skeptical of CISO demands. By developing a deeper understanding of organizational goals, the CISO gains credibility and is able to build relationships with other department heads.

This is a small step, but it is critical to create enterprise-wide understanding of cybersecurity initiatives and why they are necessary.

The path of the CISO is still an uncertain one, but developing the role in the enterprise will be critical. The volume of cyberattacks is moving in one direction, and the bad actors of the world never seem to rest. There is work to be done by boards and CISOs to ensure that qualified experts are enacting responsible cybersecurity policies throughout organizations. Cooperation between the two is necessary to ensure strategic business and cybersecurity objectives can function together. Without it, all enterprises face an increasingly serious risk.

About the Author

Julian Waits is president and chief executive officer for ThreatTrack Security. He is responsible for establishing and executing the company's go-to-market strategy, and leading all aspects of its operations.

Julian is an accomplished chief executive, business development professional, risk-management strategist and sales leader with a tenured background in information security. He also has extensive experience in the venture capital arena, leading tech companies through periods of rapid growth, innovation and transition.

Julian most recently served as the general manager of GFI Software's Security Business Unit, where he was responsible for honing the company's security product strategy and used his background in strategic development to help build a robust set of end-to-end security solutions.

He has more than 20 years of experience at all levels of IT, from network engineer to sales and previous roles as CEO, when he led Brabeion Software Corporation, maker of IT governance, risk and compliance software, and Way2Market360 LLC., a startup accelerator. He also held senior leadership positions at Archer Technologies, e-Security and BNX Systems.

He is an alumnus of both Loyola University of New Orleans and Xavier University.

The Comprehensive Approach To Securing Websites

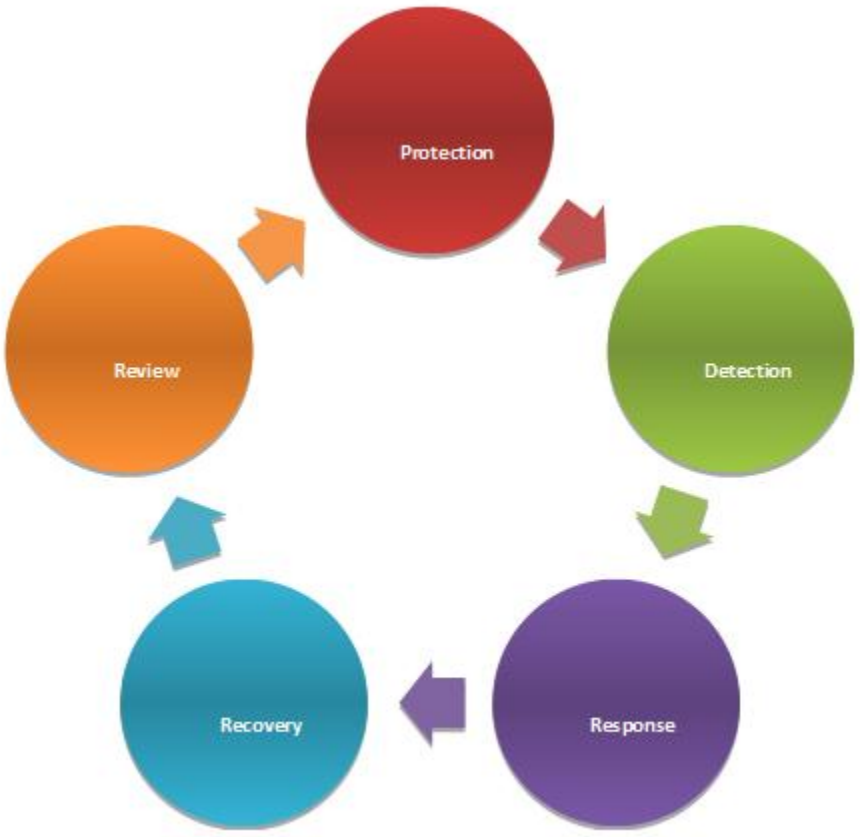
No website is an impenetrable fortress. Ad-hoc security measures are not good enough.

by Matthias Chin, Founder/Director, Banff Cyber Technologies Pte Ltd

The integrity and security of official websites are very important because they represent the reputation and trustworthiness of organizations. Incidences of website-attacks may shake the confidence of investors and customers towards that organization. Thus, protecting and preserving corporate websites should be a priority for all.

According to Zone-H, an archive of defaced websites, there are 60,000 to 120,000 of website defacement incidents every month on a global scale. Many organizations may not be aware that their websites are vulnerable to malicious threats and hacks, thus making them easy targets for vandalism or cyber-thefts.

Even for organizations that are aware of the need for securing websites, efforts towards cyber security can often be ad-hoc or patch-work. A comprehensive approach is needed to be able to guard against and respond swiftly to cyber threats effectively, and the steps involved in this cycle are explained further in this article.



1. Security

review

The first step in securing websites is to conduct a thorough review to identify security loopholes. This can be done by using security scanning tools or hiring expert security consultants to review the websites. Loopholes identified through this step should be fixed up as soon as possible. Security reviews should be scheduled and carried out at least once every six months.

2. Protect

After the security review, measures should be put in to protect the website. It is important to have web application firewalls(WAF) in addition to network firewalls. WAFs provide filters that apply a set of rules to an HTTP conversation. WAFs are able to detect and prevent common "Layer 7" web application attacks such as cross-site scripting (XSS) and SQL injections.

3. Detect

No protection is foolproof, especially since cyber threats morph very fast, and hacking methods are ever-changing. Therefore, it is important to have a proactive detection mechanism in the unfortunate event that the website is defaced or breached. Sometimes, defacement to a website is first detected by external parties, such as members of the public or a customer, before the internal team gets wind of it. Such a situation could be a major embarrassment and could do damage to reputation of the organization. Thus, proactive monitoring will allow the organization's security team to act quickly before external parties discover the security breach, so as to maintain a good reputation. Monitoring and detection can be done manually, by having someone to scan web pages on a regular basis. There are also automated softwares that can help to scan websites, and provide reports, as frequently as every few minutes.

4. Response and Recovery

Organizations need to work out an incident response and recovery plan before a website defacement or security breach happens. Such "crisis management plans" could include backing up web servers, creating temporary landing pages, etc. It is important to note that security vulnerabilities should be remedied before restoring websites from backups, so as to prevent repeat incidences of the same type of security breaches. The affected organization can consider having secure temporary landing pages on stand-by. This way, the organization can consistently show a decent corporate website, even in the face of attacks, and have time to do back-end incident handling and forensics processes.

After the "response and recovery" stage, the organization should go back to the first step of doing a "security review", so as to plan for and prevent future attacks. Thus, the job of securing websites can be done effectively, if it is viewed as a continuous process of ongoing activities mentioned above.

Many organizations tend to have lax security-controls in place for websites, as different groups of people (e.g. marketing department, managers / administrators, webmaster, etc.) are able to make changes to the corporate website. It is thus important to get these personnel to work closely with the IT-security team to have a tight change management process. The combination

of people, process and technology will always provide the best combination of security against attackers.

About The Author

Matthias Chin is the Founder and Director of Banff Cyber Technologies Pte Ltd, based in Singapore. After more than 10 years in the corporate world, Matthias took a step of faith to come out to start his own business. He wanted to build an organization that is fun to work in, develops people and creates solutions that makes the world a better place. Overcoming many challenges in the past 2 years, he has led Banff Cyber to create and launch a patent-pending cyber-security product that is widely used by banks, telcos, government agencies and Forbes Global 2000 companies. He aspires Banff Cyber to grow to be a global company that lives out the values of courage, integrity, passion to solve problems, and innovation.

Matthias has a wealth of experience in the networking and cyber security industry with 15-years of relevant experience. He possesses CCIE (Cisco Certified Internetwork Expert), GCIH (GIAC Certified Incident Handler) and CISSP (Certified Information Systems Security Professional) and has also worked in various roles of networking and security in companies such as Pacific Internet and Singapore Computer Systems.

Matthias also has strong business acumen gained from his EMBA (Helsinki School of Economics) and his experience in managing a profit centre during his time in ST Electronics. He also holds BASc (Hons), Electrical Engineering from University of Toronto.

Matthias can be reached online at enquiries@banffcyber.com or sg.linkedin.com/pub/matthias-chin/6/339/13b and at our company website http://www.banffcyber.com/

Malwarebytes' Growth Accelerates in Hot Anti-Malware Market

Founded by 18-year-old, company last year saved more than 250 million computers from advanced malware and is now protecting some of the world's largest businesses from sophisticated cyber-threats

Entering a crowded market dominated by large corporations and fighting a rash of sophisticated malware outbreaks, Marcin Kleczynski founded anti-malware company Malwarebytes in 2008. Just 18 years old at the time, he had already formed a firm determination to fight the scourge of malware on all fronts.

Just four years earlier – at 14 – he had been working part-time in his local computer shop. Noticing that numerous computers were infected with malware, despite being equipped with anti-virus software, he worked on a sample at home and, after three days of intense development, built an application to remove it. Following this, he dedicated 60 hours per week for the next four years – on top of his full-time studies – to build free software to help people remove problem malware. His development efforts were entirely transparent; Kleczynski continually sought feedback from online forums and even recruited forum members who would eventually become part of the management team.

His first creation, RogueRemover, which he designed to thwart the theft of credit card information, formed the basis for the company's first commercial product, Malwarebytes Anti-Malware. Malwarebytes Anti-Malware quickly became a popular download for consumers who wanted to complement their anti-virus software, which cannot catch all the latest threats. The product's goal: to expunge today's more sophisticated infections.

Kleczynski Named Entrepreneur of the Year by Ernst & Young

Today, Malwarebytes is a world-class organization with products protecting both consumers and businesses from today's advanced cyber-threats. With more than 140 employees around the world, the home product has over 300 million downloads and Malwarebytes' enterprise offering is used by thousands of businesses as a defense against today's sophisticated cyber-threats. In June 2014, Kleczynski's success was lauded by Ernst & Young, which named him Entrepreneur of the Year. The annual award recognizes outstanding innovation, dedication, and results in bringing new products and services to market. Just a month later, on July 10, Malwarebytes received $30 million in Series A funding.

Six years earlier, nobody could have predicted such performance and industry attention. At the launch of the fledgling Malwarebytes in 2008, many thought a bootstrapped start-up would struggle to gain share in a market dominated by large corporations. After all, Kleczynski's competitors had collectively spent billions of dollars convincing people they stopped every threat, and that there was no need for a complementary solution. Kleczynski saw this challenge as an opportunity to differentiate, targeting a tech-savvy audience who knew this to be untrue,

and he reinvested every cent of profit targeting this weak point. This counter-intuitive strategy paid dividends, and today a massive proportion of the company's business comes from personal referrals and inbound leads. Said Criss Rathbun, IT Manager, NextGen Healthcare Information Systems: "My team would routinely see machines that took four or more hours to disinfect and repair, or to simply extract, data files. I've tried dozens, if not more, removal tools. The only one that consistently cleaned a machine to a usable state was Malwarebytes. And that was using the freeware standalone version."

Kleczynski knew he had to learn from the opposition – in this case, malware developers. Known for their renegade activities, cybercriminals are unburdened by rigid power structures and organizational politics, giving them a purity of focus to develop cutting-edge techniques. Kleczynski recognized that anti-malware developers must operate in the same way, and he has placed the highest priority on allowing his employees' passion for problem-solving to come to fruition, promoting innovation over structure. In addition, he realized that good ideas are not limited to his own staff; actively courting feedback from forum users and building this into products.

The pedigree of his staff – not just executives, but also developers, support staff, and front-line personnel – has become a measure of Kleczynski's dedication to his customers. His team's innovations saved over 250 million computers last year and have removed over five billion pieces of malware.

In a recent recruiting piece for the company, Kleczynski left nothing unsaid about the passion his team has: "You should HATE malicious software in all its forms and feel a vindictive pleasure as you join us in slaughtering it." In an odd or misguided sense of loyalty, a number of cybercriminals have even been caught using Malwarebytes' technology as a benchmark for their operations.

Kleczynski Finds the Revenue Sweet Spot

Due to this passion to protect Internet users, Kleczynski is dedicated to offering much of the company's intellectual property for free. Conventional wisdom holds that a free product can build a loyal user base but may or may not induce users to "buy up" to greater capabilities. However, by leveraging the company's sterling brand and reputation, Kleczynski has launched a fee-based consumer product and a fast growing enterprise offering, which is on track to generate significant revenues this year.

As validation of the efficacy of the company's products, Malwarebytes in June, 2014, won the applause of AVTest, an independent IT-security institute, for being the only product to achieve a perfect 100 percent score for cleaning-up the latest sophisticated threats over a grueling 10 month period.

Although he has undertaken a number of philanthropic initiatives, Kleczynski says his greatest charitable donation is to “provide free malware protection,” a commitment the company has made to the Internet for life.

About the Author

Gary Good, Vice President, Trainer Communications
Email: gary@trainercomm.com

With more than 25 years of experience in security and enterprise networks, Gary Good has developed incisive profiles, white papers, and case studies of scores of category-leading start-up and emerging-growth companies. He has also documented industry breakthroughs by leading technology companies in security, cloud computing, virtualization, and software-defined networks. At Trainer Communications, he directs communications teams helping to inform industry about some of the most complex but progressive technology developments. He holds a bachelors degree in technical communication from the University of Washington.

Future Forces®
CONFERENCE & EXHIBITION
INTERNATIONAL

presents

FUTURE CRISES

FUTURE CONFLICTS, RISKS, CHALLENGES AND BUSINESS OPPORTUNITIES

Executive Guarantor AFCEA Czech Cyber Security Working Group

1st Day – DEFENCE & SECURITY DAY
Future threats, military cooperation and future challenges
Building a perspective of the future armed forces
Security policy and military strategy in a dynamically evolving international environment
Cyber defence strategy now and in the future

2nd Day – SECURITY DAY
Crisis management as a way to cope with threats and disasters
Future business opportunities in security and crisis management
Status of critical information infrastructure identification in the Czech Republic
How subject of the critical information infrastructure can prepare for new cyber security law?

3rd Day – CYBER SECURITY DAY
Cyber security visions & challenges
New cyber security strategy & legislation framework
Cyber education and international cooperation
Examining active cyber defence in deterrence and conflict escalation
Future threats, expected solutions and potential business opportunities

Main Speakers

Mr. Robin "Montana" WILLIAMS, CWDP, Chief, National Cybersecurity Education & Awareness Branch, Dept of Homeland Security
Mr. Dušan NAVRÁTIL, Director, National Security Authority of the Czech Republic
General Petr PAVEL, Chief, General Staff of the Czech Armed Forces
Mr. Ernest L. MCDUFFIE, Ph.D., Lead for the National Initiative for Cybersecurity Education (NICE),
Prof. Radica GAREVA, Ph.D., State Adviser for Communication Systems Management, Ministry of Defence of Republic of Macedonia
Mr. K. Harald DRAGER, President TIEMS
MGen. Thomas FRANZ, Deputy Chief of Staff, CIS and Cyber Defence, SHAPE (TBC)
LGen. (Ret.) Rober SHEA, USMC, President, AFCEA International
BGen. Miloš SVOBODA, General Directorate, Fire Rescue Service of the Czech Republic
Mr. Adnan KULOVAC, M.Sc., Head of INFOSEC – CIS security department, Ministry of Security, Bosna & Hercegovina
Col. Daniel MIKLÓS, General Directorate, Fire Rescue Service of the Czech Republic
Mr. Tomáš KLAČER, MERO Czech Republic
Mr. Piotr PLUTA, CISCO Systems
Mr. Robert KOSLA, Regional Director, Public Safety, National Security, Defence, Microsoft Central and Eastern Europe HQ

15 – 17 October 2014

PRAGUE, CZECH REPUBLIC

Microsoft · cisco · hp · sefira · McAfee An Intel Company · secunet · simac · Check Point · Tabernus · DSIA

www.natoexhibition.org

Briefly about Cyber Security Metrics

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

Recently I have been watching two very interesting webinars at BrightTALK - Defining Cyber threats: Understanding is the Key to Defense and The State of Metric Based Security. Afterwards I have done some research regarding what I have learned through those presentations and here I would like to explain what cyber security metrics are all about. In general, cyber metrics are exactly what the titles of the webinars suggest. They are great stuffs because they can support us in controlling, understanding, and, in case of threat, defending a cyber system. So, let's start our discussion.

What Would be Cyber Defense Goals?

With a development of cyber systems, there were a lot of requirements that had to be satisfied in terms of cyber security. As the most important cyber defense goals, some authors mention the following things: (1) increase of the cost to an attacker, (2) increase of the uncertainty that an attack would be successful, (3) increase in a chance of the detection and attribution. So, let's explain these goals.

First, let's try to explain what the cost to an attack would be. In general, this cost can be defined as a combination between: 1) the number of times a particular phase of the attack is attempted and 2) the amount of time that is spent in the preparatory phases of an attack. In other words, a cyber security is good if there is an increase in this quantity.

Further, the uncertainty that an attack could be successful can be measured as a function of the amount of time a threat spends executing its goal. If that time increases, we can say that our cyber defense is good.

Finally, the probability that a cyber attack is detected is proportional to the time the attack spends actively searching and executing its goal. We can say a cyber defense is successful if there is an increase in this quantity.

The Difference between Metrics and Measurements

First of all, let us try to understand what the metrics really are. Metrics are very often correlated with measurements, so let us see what would be a difference between these two. In general, a measurement is like a scalar. It provides single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. They are more like vector variables. In addition, measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data. That means metrics can provide us with some intelligence although they are a collection of data with some analysis applied. They are always affected by human factor, since, by definition, their interpretation depends on human's decisions.

Good metrics are usually those that are *SMART*, i.e. *specific*, *measurable*, *attainable*, *repeatable*, and *time-dependent*. The purpose of good metrics is to indicate the degree by which

security goals should be met and to drive actions in order to improve an organization's security program which would be effective and based on the best industrial practice. All these are crucially important because security metrics can be seen as a key factor in controlling, understanding and very often defending a cyber environment. They support us with a great insight into state of cyber system and allow us to develop good defense mechanisms.

Why Generating the Metrics is so Challenging?

Well, why would be so difficult to generate the metrics? Maybe because it's quite hard to determine how secure some organization is. Why would these be a problem? First of all, many would agree that the number of successful attacks cannot be an indicator how some organization may be secure. So, how can we know something is secure? Well, that depends mainly on luck. But, how would we measure luck? This question leads us to make an analogy with security metrics. It's also that complex and challenging to measure cyber metrics as it is hard in case of luck.

When we measure security metrics, we deal with very abstract terms such are asset value, threat and vulnerability. It's very hard to define and express through numbers all these quantities. For instance, asset value is the easiest of these three elements to measure. But, certain aspects of value, such as a company's good reputation, are hard, if not impossible, to quantify. On the other hand, some believe that threat cannot be measured at all, since it is the potential for harm. Some progress is being made in objectively measuring vulnerability , at least for specific types networked computer devices. Measurements of other facets of vulnerability, such as degree of understanding of security issues among computer users, remain somewhat subjective. All these is pretty difficult because security metric is still a quite young area and there is still a significant lack in the development of useful security metrics programs and strategies. There are already some data and practical experience regarding that pioneering field, but we still miss a good metrics model which would explain us how to deal in order to better understand a cyber risk.

How to Build your Security Metrics Program?

The simplest answer to this question is to follow the best industrial practice. Let us mention what all these would include. There is a lot of literature regarding this topic, but we would like to point to SANS's Guide to Security Metrics as one of the best industry guidelines in such a field. So, let's list the steps as follows:

(1) Define the metrics program goal(s) and objectives,
(2) Decide which metrics to generate,
(3) Develop strategies for generating the metrics,
(4) Establish benchmarks and targets,
(5) Determine how the metrics will be reported.

This five-step methodology should yield a firm understanding of the purpose of the security metrics program, its specific deliverables, and how, by whom, and when these deliverables will be provided. In this article, we would not go deeper into analysis of these steps.

Conclusions

In conclusions, the task of developing a security metrics program may seem daunting to some, but it need not be. The presented methodology can guide development of very simple metrics programs, as well as highly ambitious ones. In fact, the majority of cyber experts recommend organizations to make a simple start in case of security metrics. They advise managers to do what is easy, cheap, fast, and leverage existing measures and metrics. What everyone should keep in mind is that the purpose of metrics is to make improvements in a security metrics program and to assist in proving the value of that program to the organization as a whole. If a metrics program can do these, then we can say it's successful and purposeful.

About The Author

Since Milica Djekic graduated in Control Engineering at Univestity of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Currently, she's the Editor-in-Chief of Australian Science Magazine, as well as an Online Marketing Coordinator for Dejan SEO. Milica is based in Subotica, Serbia.

Put Your File Transfers... Under LOCK & KEY

- SIMPLIFY
- AUTOMATE
- ENCRYPT

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

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

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by LINOMA SOFTWARE

SEE FOR YOURSELF

Find out why this grocery chain depends on **GoAnywhere™** to automate and secure daily file exchanges with vendors.

Best Security Practices for Data Recovery

Managing the risk of a data breach in today's environment of mounting digital threats on assets and proprietary data is an ongoing battle for many businesses. The Ponemon Institute's 2014 Cost of Data Breach study found that the average cost of an organization's single data breach is $5.9 million. While most businesses have a dynamic, layered security practice in place, third-party data recovery vendors continue to be the exception.

There are many reasons businesses need to protect themselves from a possible data breach via third-party data recovery providers. Besides the loss of private information (both company and customer), the cost of a data breach can be devastating to any company.

DriveSavers has compiled best practices for businesses to implement for protection and to close the security gap in the data recovery process.

1. Gap Analysis

An internal inventory must be conducted to determine if a security gap exists within an organization. A company should be able to answer the following questions:

a. When a storage system fails, is the drive sent to a data recovery vendor?
b. Is an incident report filed?
c. What is the data recovery vendor selection criterion?
d. What is the current audit and assessment process for third-party data recovery vendors?

2. Internal and External Policy Revision

Once a security gap is identified, internal procedures should be revised accordingly to include business continuity, disaster recovery and incident response plans. Additionally, updated external policies should be applied to all third-party data recovery vendors handling the organization's sensitive or regulated data.

3. Maintain Enforcement

Revising policy, procedure and practice to mitigate the gap is the first step. However, companies must ensure enforcement of internal and external policies through mandatory annual security reviews and employee training deployment.

4. Vet Any Incoming Third-Party Data Recovery Providers

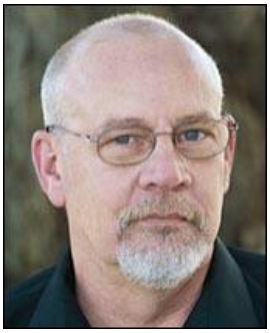
Any certified data recovery vendor should have up-to-date documents from a third-party security auditing company that comply with SOX and GLBA. An SOC II Type 2 certification, for example, satisfies these and several other regulations. In addition, the SOC II Type 2 certification requires background checks for all employees prior to employment. Data recovery, after all, is the perfect vocation for identity thieves and other criminals.

The following criterion should be used:

- Proof of internal information technology controls and data security safeguards, such as annual SOC 2 Type II audits
- Training and awareness programs for employees to ensure sensitive and confidential data is protected
- Engineers trained and certified in all leading encryption software products and platforms
- Proof of Chain of Custody documentation and certified secure network
- Vetting and background checks of all employees
- Secure and permanent data destruction when required
- Use of encryption for files in transit
- Proof of a certified ISO Class 5 Cleanroom

By implementing these four steps, companies can protect themselves against a data breach by closing the security gap in the data recovery process. With a thoroughly vetted data recovery company as part of the security protocol of a business continuity, disaster recovery and incident response plan, companies are able to act quickly and securely in the case of an unexpected data loss emergency

About the Author



As Chief Information Security Officer (CISO) and Director of eDiscovery and Digital Forensics, Michael Hall directs and implements policies and procedures concerning the privacy and security of all data received at DriveSavers, including highly critical data from government agencies, major corporations and research laboratories. Hall was instrumental in helping NIST, FDIC, OTS and BITS identify the risks of improper screening of data recovery providers.

In his previous role as Director of PC Engineering, Michael developed security protocols to handle critical and encrypted data for corporate and government accounts. He also developed and managed the ISO Class 5 certified Cleanroom, the largest and most technologically advanced in the data recovery industry. Hall has over 17 years experience in data recovery technology, focusing on high-end arrays, and has successfully recovered data from over 15,000 storage devices. Michael Hall has been trained and certified by the leading encryption vendors and is a certified eDiscovery and forensic investigator. Prior to joining DriveSavers in 1995, Hall was a Data System Engineer for the U.S. Navy. His responsibilities included computer hardware and software support for Intelligence Gathering Platforms.

Why the NGFW isn't enough

According to an Online Trust Alliance (OTA) report released in January 2014, last year broke records in terms of volume of cybercriminal activity. From stolen social media passwords and credit card data, to a breach at the Federal Reserve nearing 740 million exposed records, businesses suffered and customers lost millions of dollars. However, the OTA also reported that 89 percent of those attacks could have been avoided had security better practices been implemented on top of more traditional security plans such as next-generation firewalls.

These commonly used security measures attack threats as they are approaching, but are still lacking in full protection as threats are still able to bypass networks. Because of this, IT faces challenges as most organizations use next-generation firewalls as its only network security protection. We will explore why next-generation firewalls are not enough to fully secure networks by providing an overview on what it does and what it fails to do in order to provide protection.

Next-generation firewalls are a threat-based approach in detecting and blocking attacks by implementing security policies at the application level, as well as at the port and protocol level. They only stop attacks as they come in, and in some cases, this might mean it is too late to stop the attack.

Since a threat-based approach is only effective if potential attacks can be clearly understood, this effectively creates a big blind spot for the IT department. As a result, IT is unable to adequately address attacks, if they are unknown or undefined. This is why a next-generation firewall is not enough to sufficiently protect a network.

By adding another layer of security technology to a next-generation firewall plan, IT could strengthen its network and address advanced threats that next-generation firewalls are unable to detect and thwart in time. In order to achieve this, IT would need to implement a solution that catches suspicious behavior that isn't yet categorized or picked up as a "threat" to attack.

If IT is to eliminate this lack of visibility and provide better security measures, organizations should look to combine best practices with built-in intelligence as an added layer to its existing next-generation firewall solution, otherwise known as an intelligent next-generation firewall.

A few benefits of implementing an intelligent next-generation firewall include:

- Functionality – With proactive monitoring, enterprises can ensure far fewer service interruptions, and if the health of the network should change, then administrators are immediately notified to take action.

- Data collection – In addition to real-time threat monitoring, ongoing data collection and statistical analysis enables enterprises to quickly detect abnormal network and application traffic behavioral patterns sooner.

- Data mining – Statistical analysis, correlation analysis and machine learning are employed to review historical data to help determine key anomalies and assess whether a security alert is required.

- Multiple access evaluation – Processing the risk that can come with multiple intranet users, hosts and services allows enterprises to more efficiently and effectively assess and score harmful attacks.

- Early detection – Through robust network behavior analytics, enterprises are able to premeditate the threat, and are better prepared to mitigate issues in a timely manner.

These built-in intelligence features will further support IT in the overall need for risk analysis when it comes to catching the unknown in time before it becomes an attack to the network.

With new vulnerabilities continuing to surface and hackers becoming ever-more sophisticated, enterprises need to acknowledge that there are unknown threats that need to be identified as a precautionary action to avoid security breaches. By doing, they need to adopt more robust security measures that provide constant monitoring and data analysis to that are responsive enough to secure networks from known as well as unanticipated threats.

Customers look for solutions that address a full set of network and security issues and typically don't have the resources nor budget to purchase multiple products and management tools.

For example, Garratt-Callahan, a company with more than 275 employees and five offices located throughout the U.S. that delivers water treatment products and services facilities nationally, required a fast and reliable security solution to detect both unknown and known threats on the network. After deploying an intelligent next generation firewall, Garratt-Callahan improved network performance by reducing employee sign-on delays by as much as 15 minutes, and eliminated web application delays by 45 minutes. As a result, Garratt-Callahan benefitted from:

- Granular reporting for broader and deeper visibility into network traffic at the perimeter, including the type of attacks, the times and dates of attacks, as well as the originating source of attack

- Ease of administration and implementation of security policies

- Support bandwidth for a mobile ordering application

- Increased anti-virus depth level for increased, proactive protection

Companies like Garratt-Callahan look for solutions to address a full set of network and security issues, and typically don't have the resources nor budget to purchase multiple products and management tools. A Next-Generation Firewall is not enough, but implementing a layer of built-in intelligence provides high-performance solutions as well as deep visibility to applications and bandwidth usage to effectively help customers like Garratt-Callahan defend against network attacks.

About the Author

Timothy Liu is co-founder and CTO of Hillstone Networks. Liu has 20 years of experience in the IT industry. Before co-founding Hillstone, he managed VPN technology development at NetScreen Technologies and Juniper Networks. He has also held key engineering and management positions at Intel, Convex Computers and a few Silicon Valley startups. Liu holds a Ph.D. in Physics from University of Texas at Austin and a Bachelor in USTC. In August 2013, Liu was awarded “Top 10 CTO in 2013” by China Information World in recognition of his work in next generation intelligent security concept and data center security.

The new prototype from Germany.
Encrypted by secunet.

If you need to work with sensitive information, then come to us first. We consult, design, implement and provide guidance in all matters related to IT security. We ensure that the wrong people know only what they are supposed to know: nothing. And we take care that the right information reaches only the right people.

Sounds impossible? Put us to the test!
www.secunet.com

secunet

IT security partner of the Federal Republic of Germany

Your USB Device Can Contain Malware – How to Remain Safe

USBs have become an extremely valuable tool for use with computers. They easily allow the storage and transfer of information from one computer to any other computer. This convenient transference of data from computer to computer has revolutionized the efforts of business employees and educational students alike, allowing work files to be completed in one location and then taken to another for completion or presentation. Average computer users also find USBs to be extremely helpful for transferring files such as photos or documents from computers to other sites.

Hidden Dangers of USBs

Most people go about their days believing that they are relatively safe from harm and that malicious attacks will not happen to them. This is the same attitude that can devastate lives by malicious people bent on taking advantage of such gullibility. USB usage is a prime example. Many people are not aware that USBs can be easily infected with a variety of malware that can be carried from computer to computer. Once the USB is plugged into a device, the malware provides access to files, information and even complete control of the computer from an outside source.

Even those people who understand such dangers exist in USBs believe that they are 100 percent protected by popular antivirus software such as Norton or McAfee. The fact is that most traditional software designed for antivirus detection only search for threats in "viewable" files (those which can be viewed directly on Windows or Mac). Virus designers, however, are finding ways to escape detection by hiding their creations in the actual operational code that is used to tell the computer what to do. Currently, this area of a USB cannot be searched by antivirus software.

Types of USB Dangers

There exist a wide variety of harmful threats that can be transferred between computers via USBs. Even if a USB is infected by traditional malware that can be detected by good antivirus software like Immunet, if you do not have the software installed then such threats cannot be detected. Here is a list of potential threats that can be delivered via USB:

Malware – This is the term used to describe any illegal or questionable program that compromises the integrity of computers. Malware, viruses and other types of shady programs can cause a variety of problems from those that are simply irritating to those that are extremely severe, causing damage and great expense.

Spyware – This type of hidden program is designed to infiltrate computer systems and track movement codes so that where you go and what you view online can be observed by spyware operators.

Loss of Data – Some types of malware cause data to be eliminated. Depending on the infecting program, these losses can be minor or major.

Theft of Data - Some types of malware allow data to be stolen from infected computers. Data theft can occur in limited numbers of files or entire databases can be compromised. Malware that steals data, such as personal information, is a large contributor to the extensive rise in identity theft.

How to Prevent USB Infection

One of the most important steps in preventing USB infection is to use antivirus software on all computers that will receive the device. As has been noted, even popular antivirus programs are not always adequate for detecting more sophisticated malware threats.

However, by using additional antivirus software such as Immunet, which is compatible with other antivirus programs, you can add an additional layer of protection to your systems. The advanced technology of Immunet allows for much deeper and broader coverage so that the risk of malware and virus infection is minimized.

Once you have Immunet installed on your system, either as standalone protection or as complimentary added protection with other software programs, there are several steps you can take to help maximize protection. For example, you should block USB access to a computer if suspicious user activity has been detected, an end point for the USB has either allowed unauthorized access or has already been infected, or detection of unauthorized data transfer has occurred.

Further damage can be avoided by taking advantage of special antivirus software features, some of which are available with Immunet. These steps include enacting USB use notifications in real time, disabling, blocking and quarantining suspicious or detected user accounts, workstations or devices, and activating automated reporting of USB usage to determine patterns.

Other preventative methods can be used by companies with computer networks. Ensure that workstation activity logs are monitored regularly, continuously monitor all workstation equipment ports for USB usage, include an automatic mechanism that disables any USB drive of a workstation that has been infected, and ensure that immediate alerts are generated for unauthorized USB security breaches.

About the Author

Peter Davidson is a business analyst who loves to share entrepreneurship and marketing secrets with the world. Overcoming business challenges is his passion and he aspires to reach at the highest rung of this field.

Today's Wolf of Wall Street: Electronic teeth and a bigger appetite

By Troy Gill, AppRiver

Countless individuals around the globe maintain and rely on email, so what better place for cybercriminals to target?

There are many threat vectors used to generate wealth on the Black Market. Email-borne attacks, for example, come in the form of phishing, spear phishing, Trojans, malicious attachments and hidden scripts. All techniques constantly evolve and quickly adapt to the changing technological landscape in order to stay ahead of security professionals.

But even with the most sophisticated tools at their disposal, attackers have found success using age-old tricks.

Earlier this year, we blocked a massive "pump-and-dump" stock spam campaign that attempted to infiltrate inboxes. If you are unfamiliar with the scam, it goes something like this – scammers buy shares in a penny stock (usually costing less than $1 per share) and once they have taken a position on price they will send massive amounts of spam to users around the globe in order to generate interest in the stock. Believe it or not, there are plenty of unsuspecting people who are willing to make stock purchases based on a "tip" they receive from a source as suspect as an unsolicited email. Once real investors buy shares and "pump up" the stock price, scammers will then "dump" their shares and reap the profits.

This pump-and-dump scheme might sound familiar since it's nearly indistinguishable from the plot of Hollywood's blockbuster movie, "The Wolf of Wall Street." The only difference here is that scammers use electronic communication and not cold calling techniques.

Digital Teeth

In April 2014, spammers started using the name Oakmont Stratton in the 'From' field of their correspondence. Did you just catch the striking resemblance to the firm name Stratton Oakmont, which appears in the recent Scorsese film? We couldn't help but wonder if those scammers pulled inspiration from the film and felt compelled to impersonate the name. Either way, cybercriminals never fall short on creativity when it comes to piquing public interest.

In one campaign, the sender's address and message details changed several times a day to avoid detection. (One variation, for instance, referenced "JtMorgan" so to mimic the reputable financial services firm JP Morgan.) The spammers' stock du jour was pitched for much longer than average since they used a remarkable amount of variables in the generating algorithm to create enough unique versions of the message for the campaign to run several days.

We quarantined over 400 million of these messages over the course of the campaign that lasted 10 days.

In another campaign, spammers pushed Rainbow International Corporation (RNBI) stock. Depending on who you ask, Rainbow International Corp. is either a mining operations company in Turkey, an organization that distributes boxes and bowls or a company trying to break into the hemp industry. Either way, the company's stock was pushed into the spotlight. Spammers bought RNBI stock on or before June 24, 2014 for about $0.13 per share. A botnet, millions of pieces of spam and a short time later the price nearly doubled to around $0.23 per share.

Safety Tips

The SEC has gone after traders who deal with falsely inflated stock scams, but a simple rule of thumb is never taking action on the content of unsolicited emails. This includes clicking links, opening attachments or in this case, making investment decisions.

Also, stay away from questionable websites and make smart choices when navigating from search engine results to web pages. Cybercriminals know how to make their malicious sites appear near the top of your search results and use this tactic more often than you think. It's a good standard practice to delete unsolicited email, especially if you are unfamiliar with the sender or the sender appears to be forged.

Make sure your computer's software remains up to date, and go ahead and uninstall unused software programs from your computer because all too often they become forgotten, unpatched and create yet another target option for attackers.

Remember, a multi-layered approach to security is smart – use a properly configured firewall, anti-virus, email and web filtering products from a reputable security company and most of all, remain vigilant.

About the Author

Troy Gill is a Manager of Security Research at AppRiver. Gill is primarily responsible for evaluating security controls and identifying potential risks. He provides advice, research support, project management services, and information security expertise to assist in designing security solutions for new and existing applications.

Does mobile increase security risk for EHRs?

Electronic health records (EHR), digital versions of a patient's paper medical chart, offer medical professionals real-time access to patient records. In the past, these records were typically accessed through desktops or laptops, but as technology progresses we're seeing medical professionals increasingly accessing these important documents on mobile.

There are pros and cons to accessing EHRs on mobile. Mobile EHRs provide doctors and patients with the ability to review medical records regardless of their physical location, as long as they have access to their mobile devices, enhancing quality and convenience of patient care as well as patient participation in their own care. Mobile access to EHRs raises many security questions: Does mobile leave personal patient medical information at risk because it takes patient data outside of hospitals and doctors offices? Will mobile increase data security risk of EHRs?

Mobile Device Risk vs. Stationary Device Risk

The risk of EHRs is relative to the context of the mobile device usage. The main difference is that the mobility of the device, and the resulting risk of loss, misplacement or theft are mobile security concerns not relevant on a desktop or laptop. Microsoft and Apple provide monthly security updates to their operating systems, to fix newly uncovered security flaws because desktops are a constant source of security issues. In fact, malware and viruses are more prolific for desktop systems, simply because it's a more mature ecosystem than mobile. More threats and risks exist for desktops than for mobile, but the maturity of security controls and risk management understanding is better suited for classic desktop deployments (since they've been around for 20 years).

Due to growing popularity and the high profile nature of security issues, mobile devices are often under public scrutiny. However, these types of issues are no different than those on the desktop. The problem always comes down to who manages the device, what software is loaded on it and how the device and applications access data. Users and employees are actually the weakest link of enterprise security. They misplace devices, use weak passwords, fail to log out of workstations, share information inappropriately and unintentionally, exposing organizations to more risk through errant actions. They can also be bribed. Many organizations try to employ technology controls to overcome these problems, however the issue lies within the security policies and communication.

What's the solution?

The security of mobile EHRs is only as strong as the application responsible for downloading and viewing the EHR. The application may leverage services provided by the device to keep EHR data safe. In which case, the application needs to verify the mobile device still maintains its security integrity and can be trusted to safely house EHR data. The application needs to be a

player in the overall risk management program, and to include technical verification controls to confirm the device continues to be trustable for handling EHRs.

In the end, many wonder if healthcare institutions should limit which devices can access EHRs, in hopes of improving security. In reality, reducing variability and controlling environmental factors can certainly make for a more successful risk management program, but that comes at a cost: how do IT folks make those decisions on which devices to trust? How do they determine what they are dealing with? Increased ecosystem/environmental control can be advantageous, but only with the correct limits. If institutions limit the use of mobile devices, there's a potential for a decrease in patient satisfaction and patient care.

Since each IT department has different staff skills and experience, and different capabilities in terms of technical security controls and processes, an IT department should aim toward choices that are amenable to their existing methodology to manage devices and risk. Another situational aspect to consider is whether the organization will supply and manage the devices, or if they expect users/employees to utilize their own personal devices. The choice can drastically affect the types of practical security controls and processes that can be implemented. If personal devices are used, then further considerations need to be made regarding the other types of personal applications that may be on the device, and the potential security implications of sharing a device for EHR use and personal use. BYOD and mobile access to EHRs allow healthcare employees to increase customer satisfaction and patient care. Healthcare institutions can address security concerns by implementing mobile and data security solutions that keep patient information safe.

About the Author

Jeff Forristal, Chief Technology Officer

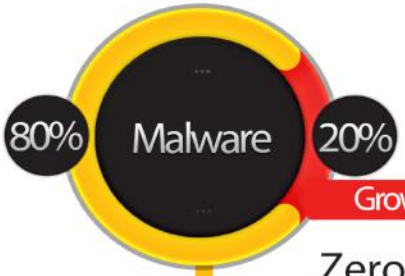
Jeff Forristal has been a security technology professional in the security industry for over a decade. His professional background includes all things security, spanning across software, hardware, operations/IT, and physical access control. Jeff has written multiple features and cover-story articles for Network Computing and Secure Enterprise magazines; he is also a contributing author to multiple books. Under the pseudonym "Rain Forest Puppy," Jeff has been recognized as an industry expert in web application security and was responsible for the first documented security discover of SQL injection, the first publicized responsible security disclosure policy, and the first intelligent open-source web application scanner. He has presented his security research in many forums, from established events like BlackHat and CanSecWest to smaller regional conferences around the world.

SnoopWall

RECLAIM YOUR PRIVACY ™

TRADITIONAL MALWARE

Virus
Blended-Threat
Botnet
Zombie
Worm
Spyware
Trojan



MODERN MALWARE

Growing by 30,000 New Samples Daily

Zero Day
Advanced Persistent Threats
Command & Control Channels
Eavesdropping
Remote Control Threats on Smartphones, Tablets, iPhones & iPads

Anti-Virus programs can detect and protect you from **Traditional Malware** and only a small fraction of **Modern Malware**

SnoopWall protects you from **Modern Malware** - puts you in control

Get SnoopWall for

Windows (COMING SOON!)

iPhone (COMING SOON!)

Android

DID YOU KNOW ?

Less spying means longer battery life for your devices!

Increase Battery life!

RECLAIM YOUR PRIVACY ™

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

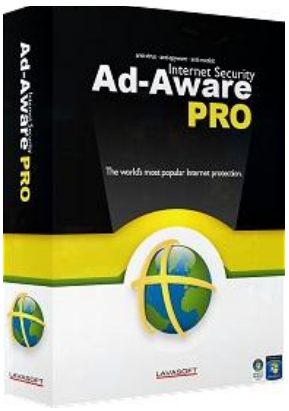
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting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

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

So use it by going here:

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

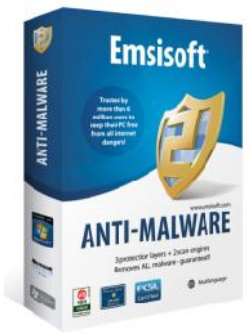
SOURCES: CDM and NAISG.ORG



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

http://register.cyberdefensemagazine.com

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



Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine September 2014

Sample Sponsors:

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

CDM
Secure Your IT World

CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

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

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS

Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for September 2014

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

Europol launches international cybercrime task force
http://www.pcworld.com/article/2600880/europol-launches-international-cybercrime-task-force.html

Leaked nude celebrity photos: When a cybercrime becomes a sex crime
http://www.washingtonpost.com/news/morning-mix/wp/2014/09/02/leaked-nude-celebrity-photos-when-a-cybercrime-becomes-a-sex-crime/

Cyber-crime awareness increasing beyond CTOs amid regulatory scrutiny
http://cooconnect.com/news/cyber-crime-awareness-increasing-beyond-ctos-amid-regulatory-scrutiny

Nude Photos Of Jennifer Lawrence And Kate Upton Leak: Five Important Lessons For All of Us
http://www.forbes.com/sites/josephsteinberg/2014/08/31/nude-photos-of-jessica-lawrence-and-kate-upton-leak-five-important-lessons-for-all-of-us/

Second Pro-Government Hacking Group 'Syrian Malware Team' Uncovered
http://www.infosecurity-magazine.com/news/government-hacking-syrian-malware/

UPS Faces Data Breach, Backoff Malware Evolves
http://risnews.edgl.com/retail-news/UPS-Faces-Data-Breach,-Backoff-Malware-Evolves95012/

NATO Set to Ratify Cyber as Key Military Threat
http://www.infosecurity-magazine.com/news/nato-set-to-ratify-cyber-as-key/

Former NSA Chief Says JPMorgan Hack May Be a Warning
http://www.bloomberg.com/news/2014-09-03/former-nsa-chief-says-jpmorgan-hack-may-be-a-warning.html

Wanted By DHS: Breakout Ideas On Domestic Cybersecurity
http://www.informationweek.com/government/cybersecurity/wanted-by-dhs-breakout-ideas-on-domestic-cybersecurity-/d/d-id/1306842

The Open Source Tool That Lets You Send Encrypted Emails to Anyone
http://www.wired.com/2014/09/oxguard/

National Guard carves out its slice of DoD cyber mission, wants teams in every state
http://www.federalnewsradio.com/241/3693882/National-Guard-carves-out-its-slice-of-DoD-cyber-mission

Computers for Hire Send JPMorgan Data to Russia
http://www.bloomberg.com/news/2014-09-04/computers-for-hire-said-to-send-jpmorgan-data-to-russia.html

In China, Cybercrime Underground Activity Doubled In 2013
http://www.darkreading.com/in-china-cybercrime-underground-activity-doubled-in-2013/d/d-id/1306921

The roots of 'Anonymous,' the infamous online hacking community
http://www.pbs.org/newshour/bb/roots-anonymous-infamous-online-hacking-community/

Holder, spy chief support Senate NSA reform bill
http://thehill.com/policy/technology/216574-holder-spy-chief-give-support-to-senate-nsa-reform-bill

Mass NSA Phone Metadata Collection in Federal Appeals Court Crosshairs
http://reason.com/blog/2014/09/03/mass-nsa-phone-metadata-collection-in-fe

Celebrity iCloud hacking turns into child abuse case over Maroney pictures
http://www.theguardian.com/technology/2014/sep/03/celebrity-icloud-hacking-turns-into-child-abuse-case-over-maroney-pictures

Linux systems infiltrated and controlled in a DDoS botnet
http://www.net-security.org/secworld.php?id=17322

Data shows Home Depot breach could be largest ever
http://www.computerworld.com/article/2601349

Are breaches inevitable?
http://www.computerworld.com/article/2601901/are-breaches-inevitable.html

The abuse of mobile-phone data
http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers

Home Depot breach a near certainty, yet Backoff remains a question
http://arstechnica.com/security/2014/09/home-depot-breach-a-near-certainty-yet-backoff-remains-a-question/

The Amazon.com of Stolen Credit Cards Makes It All So Easy
http://www.businessweek.com/articles/2014-09-04/the-amazon-dot-com-of-stolen-credit-cards-makes-it-all-so-easy

Cyber Crime Means Business- Potentially Yours
http://www.forbes.com/sites/christopherskroupa/2014/09/04/cyber-crime-means-business-potentially-yours/

Chinese Cybercrime Soars as Tools are Traded Online
http://www.infosecurity-magazine.com/news/chinese-cybercrime-soars-tools/

800 fake companies front cybercrime attack
http://www.scmagazineuk.com/800-fake-companies-front-cybercrime-attack/article/369665/

Google, Facebook ID codes found in Android malware stash
http://www.csoonline.com/article/2603022/data-protection/android-malware-stash-of-text-messages-found.html

Hackers breach HealthCare.gov server, upload malware
https://bangordailynews.com/2014/09/04/news/nation/hackers-break-into-healthcare-gov-server-upload-malware/?ref=moreInnationThumb

JPMorgan Hack Likely A Warning To 'Vulnerable' US Financial Institutions, Former NSA Chief Says
http://www.ibtimes.com/jpmorgan-hack-likely-warning-vulnerable-us-financial-institutions-former-nsa-chief-says-1676720

Privacy groups pressure Senate on NSA
http://thehill.com/policy/technology/216749-privacy-groups-pressure-senate-on-nsa

Successful Windows malware ported to Mac
http://www.zdnet.com/successful-windows-malware-ported-to-mac-7000033331/

Expert teaches UM students cybersecurity basics - lock picking
http://missoulian.com/news/local/expert-gives-um-students-cybersecurity-basics---lock-picking/article_b11ad26e-3497-11e4-a62c-0019bb2963f4.html?comment_form=true

Popular Android Apps Fail Basic Security Tests, Putting Privacy at Risk
http://english.farsnews.com/newstext.aspx?nn=13930617001453

Home Depot Hit By Same Malware as Target
http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/

Hack attacks spur calls for cyber insurance
http://thehill.com/policy/technology/216840-hack-attacks-spur-calls-for-cyber-insurance

Want to Reform the NSA? Give Edward Snowden Immunity
http://www.theatlantic.com/politics/archive/2014/09/want-to-reform-the-nsa-give-edward-snowden-immunity/379612/

NSA Reform Will Likely Have to Wait Until After the Election
http://www.nationaljournal.com/tech/nsa-reform-will-likely-have-to-wait-until-after-the-election-20140907

The FBI Finally Says How It 'Legally' Pinpointed Silk Road's Server
http://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/

Cyberespionage group starts using new Mac OS X backdoor program
http://www.csoonline.com/article/2602956/security/cyberespionage-group-starts-using-new-mac-os-x-backdoor-program.html

This Week in Tech: Lawmakers take on cybersecurity

http://thehill.com/policy/technology/216905-this-week-in-tech-lawmakers-take-on-cybersecurity

Would Pay Scales Close the Cybersecurity Workforce Gap?
http://www.defenseone.com/management/2014/09/would-pay-scales-close-cybersecurity-workforce-gap/93329/?oref=d-channelriver

Typical home to contain 500 smart devices by 2022
http://net-security.org/secworld.php?id=17336

Researchers find data leaks in Instagram, Grindr, OoVoo and more
http://www.cnet.com/au/news/researchers-find-data-leaks-in-instagram-grindr-oovoo-and-more/

The Senate must act to protect Americans from cyber crime

http://thehill.com/opinion/op-ed/217031-the-senate-must-act-to-protect-americans-from-cyber-crime

In Wake of Confirmed Breach at Home Depot, Banks See Spike in PIN Debit Card Fraud
http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/

'Undetectable' Peter Pan virus hits thousands: Malware disguised as pantomine tickets could steal your passwords

http://www.dailymail.co.uk/sciencetech/article-2749108/

25 varieties of malware aimed at Mac OS X this year
http://www.trustedreviews.com/news/25-varieties-of-malware-aimed-at-mac-os-x-this-year

Who Will Protect Tomorrow's Digital Countries?
http://www.theatlantic.com/international/archive/2014/09/when-a-digital-country-is-in-nato/379806/

WH Official: Cyber Coverage Will Be a Basic Insurance Policy By 2020
http://www.nextgov.com/cybersecurity/2014/09/wh-official-cyber-coverage-will-be-basic-insurance-policy-2020/93503/?oref=ng-skybox

Tech industry groups ask Senate to 'swiftly pass' NSA curbs
http://www.computerworld.com/article/2604421/government/tech-industry-groups-ask-senate-to-swiftly-pass-nsa-curbs.html

Report: Congress won't shut down NSA database this year

http://arstechnica.com/tech-policy/2014/09/report-congress-wont-shut-down-nsa-database-this-year/

What U.S. organizations should know about foreign state- sponsored cyberattacks
http://venturebeat.com/2014/09/08/what-u-s-organizations-should-know-about-foreign-state-sponsored-cyberattacks/

Salesforce warns customers of malware attack
http://www.pcworld.com/article/2604740/salesforce-warns-customers-of-malware-attack.html

Study: 15 Million Devices Infected With Mobile Malware
http://www.darkreading.com/study-15-million-devices-infected-with-mobile-malware/d/d-id/1315477

Let's pass cybersecurity legislation
http://thehill.com/opinion/op-ed/217151-lets-pass-cybersecurity-legislation

How a large ISP fights DDoS attacks with a custom solution
http://net-security.org/secworld.php?id=17347

DARPA is after vulnerabilities in algorithms implemented in software
http://net-security.org/secworld.php?id=17346

Home Depot breach reveals how challenging it is to ward off data theft
http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/09/home-depot-breach-reveals-how-challenging-it-is-to-ward-off-data-theft/

How Wednesday's 'Internet Slowdown' is supposed to work
http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/09/how-wednesdays-internet-slowdown-is-supposed-to-work/

How Many Contractors Run Fed IT?
http://www.govinfosecurity.com/how-many-contractors-run-fed-it-a-7297

Federal agency to end contracts of background-check contractor USIS
http://www.stripes.com/news/us/federal-agency-to-end-contracts-of-background-check-contractor-usis-1.302244

Information commissioner: 'apps are failing to respect user privacy'

http://www.theguardian.com/technology/2014/sep/10/information-commissioner-apps-failing-user-privacy-information-facebook

DOD Deputy CIO: 'Cybersecurity should vary by mission'
http://fcw.com/articles/2014/09/10/cybersecurity-should-vary.aspx

iPwned: How easy is it to mine Apple services, devices for data?
http://arstechnica.com/features/2014/09/ipwned-mining-iphones-icloud-for-personal-data-is-terrifying-simple/

Researchers analyze phishing campaign spreading 'vawtrak' malware
http://www.scmagazine.com/researchers-analyze-phishing-campaign-spreading-vawtrak-malware/article/370842/

Attackers Compromise Vulnerable Web Servers to Power DDoS Assaultshttp://www.eweek.com/security/attackers-compromise-vulnerable-web-servers-to-power-ddos-assaults.html

Ex-NSA Chief's Anti-Hacker Patent Sparks Ethics Questions
http://www.bloomberg.com/news/2014-09-10/ex-spymaster-seeks-anti-hacker-patent-drawing-objections.html

Edward Snowden Not the Only Insider Threat
http://www.afcea.org/content/?q=node/13443

Cybersecurity expert sees rising threat from 'adversaries'
http://www.heraldmailmedia.com/news/local/cybersecurity-expert-sees-rising-threat-from-adversaries/article_ba143dfc-45da-5cd3-a227-2913feadfe61.html

The Morning Download: Bidding War for Cybersecurity Experts Leads to More Pay, Bigger Budgets
http://blogs.wsj.com/cio/2014/09/11/the-morning-download-bidding-war-for-cybersecurity-experts-leads-to-more-pay-bigger-budgets/

How Online Black Markets Have Evolved Since Silk Road's Downfall
http://www.wired.com/2014/09/internet-black-market/

PayPal goes crypto-currency with Bitcoin
http://www.theregister.co.uk/2014/09/11/paypal_goes_cryptocurrency_with_bitcoin/

Air Force wants a better way to map and analyze its networks
http://defensesystems.com/articles/2014/09/15/air-force-mama-network-mapping-analysis.aspx?admgarea=DS

NIST Forensics Org Seeks Members for Digital Evidence Subcommittee
http://www.executivegov.com/2014/09/nist-forensics-org-seeks-members-for-digital-evidence-subcommittee/

New malware spreads over Twitch chat, targets Steam accounts
http://www.pcworld.com/article/2606007/new-malware-spreads-over-twitch-chat-targets-steam-accounts.html

Dragonfly malware targeting pharmaceutical companies
http://www.net-security.org/malware_news.php?id=2865

Spy court renews NSA metadata program
http://thehill.com/policy/technology/217618-spy-court-renews-nsa-program

Army Cyber Leader Touts Hacking Skills
http://www.govinfosecurity.com/interviews/army-cyber-leader-touts-hacking-skills-i-2446

New data center protects against solar storms and nuclear EMPs
http://www.computerworld.com/article/2606378/

Emerging cloud threats and how to address them
http://www.net-security.org/article.php?id=2126

The War Of Zeros And Ones
http://www.popsci.com/article/technology/war-zeros-and-ones?dom=PSC&loc=poprail&lnk=1&con=the-war-of-zeros-and-ones

This Week in Tech: Net neutrality comments close
http://thehill.com/policy/technology/217690-this-week-in-tech-net-neutrality-comments-close

Students Study a Rampant Virus at University Cybersecurity Lab
http://www.edtechmagazine.com/higher/article/2014/09/students-study-rampant-virus-university-cybersecurity-lab

Decade-long cybercrime ring hacked European banks and labs
http://www.wired.co.uk/news/archive/2014-09/16/harkonnen-operation

Biometric security: giving cyber criminals the finger
http://www.finextra.com/blogs/fullblog.aspx?blogid=9945

With MAMA, U.S. Air Force Aiming to Raise Cyber Awareness on Networks
http://threatpost.com/with-mama-u-s-air-force-aiming-to-raise-cyber-awareness-on-networks

What DHS Must Do to Expand Cybersecurity Information-Sharing
http://www.fedtechmagazine.com/article/2014/09/what-dhs-must-do-expand-cybersecurity-information-sharing

Are People Too Trusting With Their Cybersecurity?
http://www.govtech.com/security/Are-People-Too-Trusting-With-Their-Cybersecurity.html

Protecting Servers from Remote Attacks
http://www.govinfosecurity.com/protecting-servers-from-remote-attacks-a-7313

'Tiny banker' malware targets US financial institutions
http://www.computerworld.com/article/2683956/tiny-banker-malware-targets-us-financial-institutions.html

Google Piles Pressure On Congress With Latest Transparency Report
http://www.forbes.com/sites/emmawoollacott/2014/09/16/google-piles-pressure-on-congress-with-latest-transparency-report/

Hacker exploits printer Web interface to install, run Doom
http://arstechnica.com/security/2014/09/hacker-exploits-printer-web-interface-to-install-run-doom/

Turning the tables on "Windows Support" scammers by compromising their PCs
http://arstechnica.com/security/2014/09/turning-the-tables-on-windows-support-scammers-by-compromising-their-pcs/

Macro based malware is on the rise
http://www.net-security.org/malware_news.php?id=2867

Even Biometric Locks Can be Picked
http://www.dfinews.com/news/2014/09/even-biometric-locks-can-be-picked

Middle-School Dropout Codes Clever Chat Program That Foils NSA Spying
http://www.wired.com/2014/09/new-encrypted-chat-program-thwarts-nsa-eliminating-metadata/

NSA Reform Bill Splits Reformers
http://www.huffingtonpost.com/2014/09/16/nsa-reform-bill-patrick-leahy_n_5831070.html

Privacy, diversity and cybersecurity take center stage in new intel strategy
http://www.washingtontimes.com/news/2014/sep/17/hayden-privacy-diversity-and-cybersecurity-take-ce/

GAO: HealthCare.gov Has Security Flaws
http://www.govinfosecurity.com/gao-healthcaregov-has-security-flaws-a-7326

Apple turns on iCloud two-step verification after nude selfie scandal
http://www.computerworld.com/article/2683928/

Protecting Infrastructure with Smarter Cyber-Physical Systems
http://www.dfinews.com/news/2014/09/protecting-infrastructure-smarter-cyber-physical-systems

XSS bug allows Amazon account hijacking
http://www.net-security.org/secworld.php?id=17370

How to talk infosec with kids
http://www.net-security.org/article.php?id=2127

Intelligence chief says Snowden leaks created 'perfect storm'
http://thehill.com/policy/technology/218155-intelligence-chief-says-snowden-leaks-created-perfect-storm

China frequently hacks TRANSCOM contractors' computers, probe finds
http://www.stripes.com/news/pacific/china-frequently-hacks-transcom-contractors-computers-probe-finds-1.303518

Apple iOS 8 Reboots Privacy, Security
http://www.govinfosecurity.com/apple-ios-8-reboots-privacy-security-a-7331

Cybercrime in 2025: Where do you go when there's nowhere to hide?

http://www.gmanetwork.com/news/story/379822

VBA malware on rise, templates make it easier to write code
http://www.scmagazine.com/researchers-at-sophoslabs-found-an-uptick-in-vba-samples-in-july/article/372184/

The Dark Web Gets Darker With Rise of the 'Evolution' Drug Market
http://www.wired.com/2014/09/dark-web-evolution/

Is NSA Planning to Beef up Cyber Response Capabilities?
http://www.nextgov.com/big-data/2014/09/nsa-cyber-response-capabilities/94334/

US Official: Chinese Want NSA Cyber Schools. Really.
http://www.nextgov.com/cybersecurity/2014/09/us-official-chinese-want-nsa-cyber-schools-really/94382/

Apple: New iPhones can't be unlocked - even with a warrant
http://thehill.com/policy/technology/218157-new-iphones-cant-be-unlocked-even-with-a-warrant

Why kids probably don't need an actual digital sandbox
http://www.washingtonpost.com/blogs/innovations/wp/2014/09/18/why-kids-probably-dont-need-an-actual-digital-sandbox/

Senate Passes Cybersecurity Skills Shortage Bill
http://www.govinfosecurity.com/senate-passes-cybersecurity-skills-shortage-bill-a-7340

North Korea says jailed California man sought to be 'second Snowden'
http://www.stripes.com/news/pacific/north-korea-says-jailed-california-man-sought-to-be-second-snowden-1.304284

Upcoming Book Charts Anonymous' Rise, From Silly Pranks to Serious Power
http://www.wired.com/2014/09/upcoming-book-charts-anonymous-rise-silly-pranks-serious-power/

The Cyber Liability Shell Game
http://ww2.cfo.com/risk-management/2014/09/cyber-liability-shell-game/

For White House Cyber Czar, Being Called 'Total n00b' Just Comes with the Territory
http://www.nextgov.com/cybersecurity/2014/09/white-house-cyber-czar-being-called-total-

n00b-just-comes-territory/94652/

Tech moves to lock out government
http://thehill.com/policy/technology/218393-tech-moves-to-lock-out-government

James Clapper, ODNI Unveil 4-Year National Intelligence Strategy
http://www.executivegov.com/2014/09/james-clapper-odni-unveil-4-year-national-intelligence-strategy/

Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data
http://www.forbes.com/sites/lorenthompson/2014/09/19/cyber-alliances-collective-defense-becomes-central-to-securing-networks-data/

'Need To' Declassify More Cyber Attacks: NSA Deputy Ledgett
http://breakingdefense.com/2014/09/need-to-declassify-more-cyber-attacks-nsa-deputy-ledgett/

IEEE standards group wants to bring order to Internet of Things
http://www.computerworld.com/article/2686714/networking-hardware/ieee-standards-group-wants-to-bring-order-to-internet-of-things.html

HealthCare.gov audit found vulnerability
http://thehill.com/policy/healthcare/218612-report-healthcaregov-audit-found-vulnerability

US regulator raises alarm for 'Armageddon-type' cyber attack
http://www.theguardian.com/technology/2014/sep/22/us-regulator-armageddon-type-cyber-attack

Google stops malicious advertising campaign that could have reached millions
http://arstechnica.com/security/2014/09/google-stops-malicious-advertising-campaign-that-could-have-reached-millions/

College Campuses Get An "F" In Cybersecurity
http://securitywatch.pcmag.com/security/326921-college-campuses-get-an-f-in-cybersecurity

CipherShed: A replacement for TrueCrypt
http://www.net-security.org/secworld.php?id=17392

Researcher Discloses Wi-Fi Thermostat Vulnerabilities
https://threatpost.com/researcher-discloses-wi-fi-thermostat-vulnerabilities/108434

Tor users could be FBI's main target if legal power grab succeeds
https://nakedsecurity.sophos.com/2014/09/22/tor-users-could-be-fbis-main-target-if-legal-power-grab-succeeds/

Kids coding at school: 'When you learn computing, you're thinking about thinking'
http://www.theguardian.com/technology/2014/sep/22/computing-bcs-uk-computing-curriculum

The FDA wants to talk about medical device cybersecurity
http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/23/the-fda-wants-to-talk-about-medical-device-cybersecurity/

A Police Dog for the Digital Age: She Can Smell the USB Drive You're Hiding
http://www.bloomberg.com/news/2014-09-23/a-police-dog-for-the-digital-age-she-can-smell-the-usb-drive-you-re-hiding.html

European banks and Europol join forces to fight cybercrime
http://www.net-security.org/secworld.php?id=17395

Mitigations for Spike DDoS toolkit-powered attacks
http://www.net-security.org/secworld.php?id=17406

Metal Gear Online brought back to life by professional hackers
http://www.theguardian.com/technology/2014/sep/24/metal-gear-online-professional-hackers

China Hacks Expose Communications Flaw
http://www.govinfosecurity.com/blogs/china-hacks-expose-communications-flaw-p-1746

More Alarming Data on the Cybersecurity Skills Shortage
http://www.networkworld.com/article/2687381/cisco-subnet/more-data-on-the-cybersecurity-skills-shortage.html

We just might put a dent in data breaches
http://www.computerworld.com/article/2687075/we-just-might-put-a-dent-in-data-breaches.html

What is the Bash Bug computer virus and should you be worried?
http://www.cleveland.com/nation/index.ssf/2014/09/what_is_the_bash_bug_computer.html

FBI blasts Apple, Google for locking police out of phones
http://www.washingtonpost.com/business/technology/fbi-blasts-apple-google-for-locking-police-out-of-phones/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html

Crimtrac Acorn system could enable cybercrime reporting by mouse click
http://www.theguardian.com/technology/2014/sep/26/crimtrac-acorn-system-could-enable-cybercrime-reporting-by-mouse-click

How do you stop a cyber-criminal? Think like one
http://www.cbsnews.com/news/how-do-you-stop-a-cyber-criminal-think-like-one/

Russian malware used by 'privateer' hackers against Ukrainian government
http://www.theguardian.com/technology/2014/sep/25/russian-malware-privateer-hackers-ukraine

Bitcoin Miner Malware Hidden in Free Game Downloads
http://insidebitcoins.com/news/bitcoin-miner-malware-hidden-in-free-game-downloads/24866

Shellshock: How to protect your Unix, Linux and Mac servers
http://www.zdnet.com/shellshock-how-to-protect-your-unix-linux-and-mac-servers-7000034072/

Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks
http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/

U.S., China talk cybersecurity despite military hack attack
http://www.washingtontimes.com/news/2014/sep/25/us-china-talk-cybersecurity-despite-military-hack-/?utm_source=RSS_Feed&utm_medium=RSS

Do We Need to 'Disrupt' the Cybersecurity Status Quo?
http://www.nextgov.com/cybersecurity/cybersecurity-report/2014/09/do-we-need-disrupt-cybersecurity-status-quo/95150/

Ramping Up Medical Device Cybersecurity
http://www.govinfosecurity.com/ramping-up-medical-device-cybersecurity-a-7360

Shellshock DDoS Attacks Spike
http://www.govinfosecurity.com/shellshock-ddos-attacks-spike-a-7365

Crime-as-a-Service lowers entry barriers to cybercrime world
http://www.itpro.co.uk/security/23200/crime-as-a-service-lowers-entry-barriers-to-cybercrime-world

General Motors hires first cyber security chief
http://www.computing.co.uk/ctg/news/2372722/general-motors-hires-first-cyber-security-chief

Hacker Group Lizard Squad Takes Down Destiny, Call of Duty, FIFA And More
http://www.forbes.com/sites/insertcoin/2014/09/29/hacker-group-lizard-squad-takes-down-destiny-call-of-duty-fifa-and-more/

Tim Berners-Lee calls for internet bill of rights to ensure greater privacy
http://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy

Disgruntled workers pose 'significant cyber threat,' feds warn
http://thehill.com/policy/technology/218985-feds-warn-disgruntled-workers-pose-significant-cyber-threat

What Cyberthreat Does ISIS Pose?
http://www.govinfosecurity.com/blogs/what-cyberthreat-does-isis-pose-p-1747

Trust in the cloud is at an all-time low
http://net-security.org/secworld.php?id=17419

The toughest case: What if Osama bin Laden had an iPhone?
http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/26/the-toughest-case-what-if-osama-bin-laden-had-an-iphone/

Should You Say "I Don't Know" on the Witness Stand?
http://www.dfinews.com/articles/2014/09/should-you-say-i-don%E2%80%99t-know-witness-stand

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

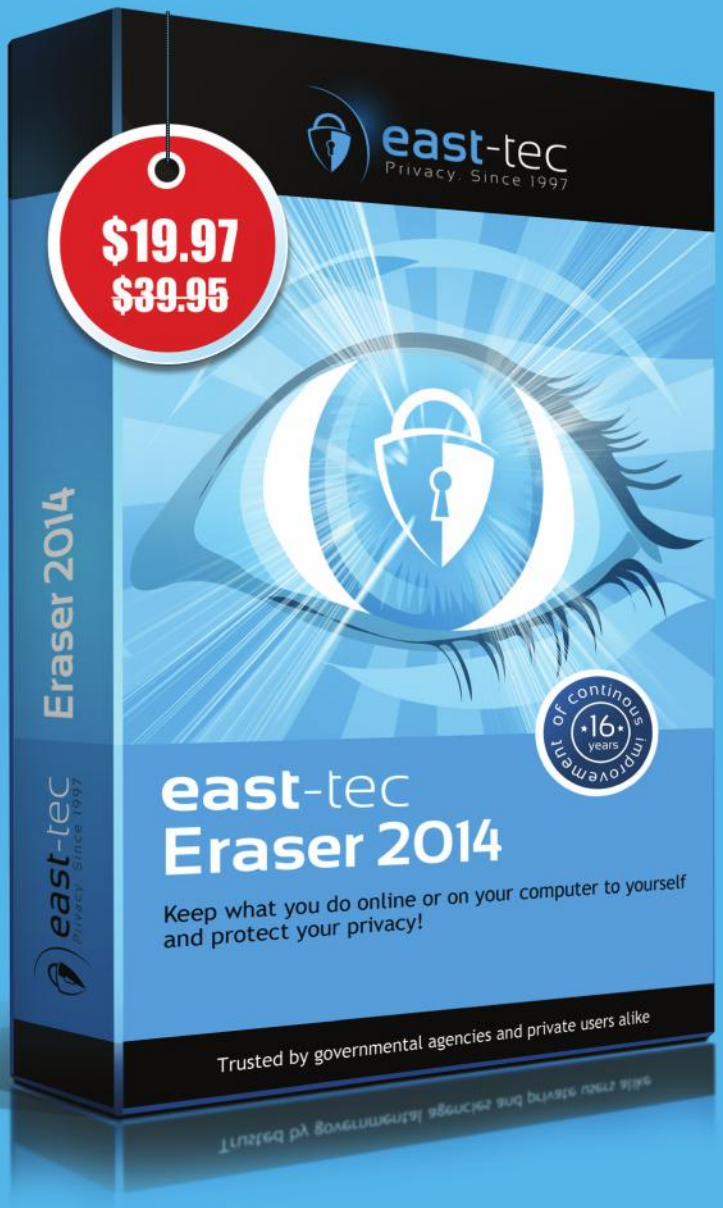
Cyber Defense Magazine - Cyber Warnings rev. date: 09/29/2014

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

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



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014