CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Critical Infrastructure Security
Cybersecurity Branding
Employee Training
Drupal Security

March 2016

MORE INSIDE!

CONTENTS

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Luis Corrons
Eric J. Eifert
Evan Goldberg
Doug Wylie
Marc Saldana
Jen Martinson
Dustin Childs
Bob Chaput
Milica Djekic
Ian Muscat
Narendran Vaideeswaran
Cherif Sleiman
Prerna Lal
Todd Helfrich

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®

Unwinding from a Spectacular RSA Conference 2016

Friends,

This year's RSA Conference broke all the records by way of number of new ventures and total attendees (we hear there were over 40,000) and we ran completely out of print editions for the first time ever, handing out thousands of copies.

As we reflect on a spectacular conference, I admit our staff felt a bit overwhelmed with so many vendors claiming to have the best Endpoint Detect and Respond (EDR) solutions. The problem we have with these solutions is that they continue down the slippery slope of reactivity to being exploited. While it's nice to quarantine an infected endpoint after the fact and try to remediate, it brings me back to our quest here at Cyber Defense Magazine – to help uncover new ways to be PROACTIVE and one step AHEAD of the NEXT THREAT. While this seems a daunting and challenging task, won't it be better to not get infected with the next piece of ransomware, than to follow the FBI's current instructions – which is to pay the ranson?

Here are some simple things most organizations are not doing, which is why the EDR market has been sparked with hundreds of millions in new investment dollars: most organizations don't ever test their backup systems; most backup systems are not run frequently enough; most systems are not protected against exploitation of CVEs (common vulnerabilities and exposures); most data is not protected by STRONG ENCRYPTION and most employees don't understand why clicking a link is such a big deal.

If we can just hone our organizations in on simple, logical procedures like better backups, testing them frequently, having a re-image system in place, ready to pounce an infected endpoint that has RANSOMWARE with a wipe, re-image, restore, we won't be paying ransom to anyone. If we have STRONG ENCRYPTION running so that our systems are already protected against data theft, then those who steal data but can't view it, won't be selling it on the black market. Yet, we continue to read about Medical organization breaches, retailer breaches, hospitality breaches, bank and credit union breaches and even US Gov breaches on a regular basis. It's time to look forward and focus on simple things to get ahead of the next threat. This won't require spending a lot of money, just finding the most innovative BREACH PREVENTION solutions on the market, BETTER INFOSEC TRAINING and TESTING our BACKUP/RESTORE process. With that said, I hope you find some additional new ideas that will help you not be the next victim, in this edition of Cyber Warnings.

To our faithful readers, Enjoy

Pierluigi Paganini

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

A Historic Year Ahead for Cybercrime

BY: Luis Corrons, PandaLabs Technical Director

Now that we're well in 2016, we have some perspective on 2015 and what an incredible year it was from a cybercrime perspective. Unfortunately, in spite of the whopping 84 million samples of new malware created last year, one fourth of all the malware in history – we're looking at continued growth and sophistication of malware in 2016. If the kind of attacks we're seeing continues, as we expect it will, 2016 will shatter even the most astounding numbers we came across in 2015.

The amount of attacks are increasing, and cybercriminal gangs are focusing on more profitable targets. Corporations, big and small have been attacked in numerous ways, but two more increasingly popular tactics are, Point-of-Sale (PoS) Trojans and Ransomware.

PoS Attacks

While we are seeing an increase in PoS attacks, it is the frequency and sophistication that are making them more prominent, but this form of cybercrime is not new. The big data breach against Target in 2013 was a result of a PoS attack, and it resulted in 46 million debit and credit card stolen in just a few weeks. In 2015, we also saw an increase in these attacks against specific business verticals, most notably, hotel chains, which experienced a slew of attacks last year.

Major chains such as the Mandarin Oriental (hotels in America and Europe); Trump Hotels (seven hotels); Hard Rock Las Vegas (shops and restaurants); FireKeepers Casino Hotel in Battle Creek, MI; Hilton, Starwood (105 hotels) and Hyatt Hotels, (254 affected hotels in 54 countries), represent a sampling of huge hospitality companies that have been attacked.

Ransomware Attacks

Ransomware is not a new threat either. We trace the first attacks back to approximately the end of 2013. However, the threat has evolved and only gotten stronger, their targets have moved away from home users, and onto businesses and corporations. When this malware gets into the system it steals a copy of the address book, to be used for future attacks.

This tactic is popular among cybercriminals for a number of reasons, but the most invasive (and oftentimes successful) is, in order to recover the encrypted files, the victim's only solution is to pay the cybercriminals directly, (unless they have an updated backup copy of the files). With nominal demands for payment (depending on the attack, the average is $300-$400), most companies will pay that to prevent the tens of thousands of dollars in losses if they don`t pay.

Cybercriminals are even resurfacing techniques from almost 20 years ago, such as the use of macros in Office documents especially Word. Most users have a false sense of security that a text document will not contain any threats. With this in mind, and being aware that the perimeter

filters do not act against such files, there has been a sharp increase in these attacks. The weak point of this attack is that the users must enable macros, yet cybercriminals have found ways around this, by successfully developing some ingenious social engineering techniques.

One example, discovered by PandaLabs, was a Word document containing a blurred image. At the top of the document in bold capital letters there was a message that indicated that the image was blurred for security reasons. If the user wanted access to the information, they had to enable the macros, with an arrow pointing to the button to be pressed.

Once enabled, it showed you the clear image while simultaneously infecting you with a type of Cryptolocker.

2016: What Can We Expect?

Exploit Kits: These will continue to be the favored tool of cybercriminals, when looking to achieve massive infections. Exploit kits can be bought on the black market, and come with updates, allowing attackers to find new victims. Many security solutions still aren't capable of effectively combatting this type of attack, resulting in a high success rate for attackers.

Malware: The number of new malware samples will keep rising. Although the majority of samples will continue to be Portable Executable (PE) types, we foresee a growth in non-PE malware, mainly scripts. It won't just be the well-known JavaScript, but rather a growth in the use and abuse of PowerShell, a tool that comes by default with Windows 10, which allows for the running of all types of scripts.

It will combine itself with known attacks such as Fileless Attacks, where, instead of the malicious code being on a physical file on the computer, it will be a parameter in the execution of a command, or an entry in the registry that contains the script to be executed.

Targeted Attacks: There will be a growth in targeted attacks. The use of rootkit techniques, which allows the attack to hide itself from the view of the operating system. Companies will be obliged to take security measures to be protected against these attacks, as they can seriously damage the company, both financially and in terms of reputation. These attacks steal both confidential company data, (financial data, strategic plans, etc.) and that of their clients.

Malware for Android: Malware for mobile devices will increase, especially for Android, the most popular operating system on the market. We will see that more threats will root the device, meaning that eliminating it will be nearly impossible for antiviruses, except for those that come installed from the factory.

Mobile Payment Platforms: It is still unclear if 2016 will be the year in which these platforms become truly popular, but what we do know is as their use increases, so will attacks from cybercriminals. If any of the platforms become the first to break through, it will become a prime candidate for attackers looking for any weakness that they can abuse in the system.

Internet of Things: We will have more devices connected to the Internet, and we will see many tests that show how different attacks can be carried out. We have already seen many tests in 2015, like those on automobile software, which allowed for the cars to be remotely controlled while travelling.

Critical Infrastructure: It won't be a target for regular cybercriminals, but when it comes to cyberwar, the power to remotely sabotage the critical infrastructure of another country is something so valued that intelligence services from the world's most powerful countries will try to achieve it. It takes a lot of money and planning to carry out this type of attack, as we saw in the case of Stuxnet.

Threat Intelligence for Businesses: The growth in the number and complexity of attacks is changing the use of information, and also how it is shared. Even though companies that offer security solutions and services usually share information to protect their clients, their set up will have to change dramatically.

We will have large companies asking their security provider to give them all of this information, while also collecting all of the information that is on their networks, and sharing it with other businesses.

It is evident that the war on cybercrime is getting more intense. The level of sophistication is unparalleled, and 2016 is going to be another banner year for both the quantity and invasiveness of attacks. No one is immune, but with the foresight, proactivity and security measures in place, consumers and companies alike can do what they can to prevent, and minimize the incredible damage that cybercriminals can inflict.

About the Author

"Luis Corrons has been working in the security industry for more than 17 years, specifically in the antivirus field. He is the Technical Director at PandaLabs, the malware research lab at Panda Security.

Luis is a WildList reporter, member of the Board of Directors at AMTSO (Anti-Malware Testing Standards Organization) and member of the Board of Directors at MUTE (Malicious URLs Tracking and Exchange).

He is also a top rated industry speaker at events like Virus Bulletin, HackInTheBox, APWG, Security BSides, etc. Luis also serves as liaison between Panda Security and law enforcement agencies, and has helped in a number of cyber-criminal investigations."

Protecting energy facilities from cyber attack

Energy companies are often targeted by sophisticated hackers looking to create disruption across national economies. Although they are a challenge to protect, there are clear procedures they can follow to both assess their risk and mitigate it.

By Eric J. Eifert, Sr. VP of Managed Security Services

Over the past few years we have witnessed a paradigm shift in cybercrime: attacks have moved from focusing on stealing confidential information for gain and reputational damage, to manipulating complex systems to produce real-world effects. Increasingly, industrial control systems are linked to the wider internet. While this has increased efficiency, enabled the collection and analysis of performance data and allowed remote maintenance, it has also left systems vulnerable to malicious interference.

Oil and gas firms, which underpin the economy of the GCC, are exposed across the full spectrum of cyber threat from loss of intellectual property and loss of their reputation, to disruption of operations. While traditional threat actors; rivals, criminals and environmental activists persist, we're seeing a concerning rise in sophisticated attacks against control systems by state-sponsored agents.

The malware programme nicknamed Stuxnet (discovered in 2010), generally thought to be the product of intelligence service cyber co-operation, targeted computers that controlled centrifuges in a nuclear enrichment programme, altering their rotation speeds, causing the centrifuges to tear themselves apart and producing a cascade of second-order effects. Ukraine also suffered a multi-tiered attack on its energy facilities in December last year.

The Ukrainian CERT reported that in total eight facilities were attacked, ultimately leading to a loss of power for 80,000 people in the middle of winter. Although most recovered their power within three hours, after-shocks continued for days with power company employees having to travel along ice-covered roads to remote sub-stations to manually close breakers the hackers had opened remotely.

Most sinisterly, the attack was multi-pronged; opening of breakers was accompanied by spoofing of monitoring systems and a distributed denial of service attack on helplines, all designed to systematically prevent the Ukrainian authorities from resuming control. Although no one has claimed responsibility for the attack, one company did manage to trace it to an ISP operated in Russia.

Energy companies are particularly vulnerable to this type of attack because of the sheer complexity of their infrastructure and their intersection with third party suppliers and contractors over whom they may have little control. Energy is a strategic target for malicious actors, as power interruptions, even if minor, can cause a cascade of secondary consequences which may cause longer term chaos.

The GCC is particularly vulnerable to the type of cascading attack as it supports millions of people in a desert environment, which in pre-20th century conditions could support only a fraction of their number. A power cut would likely cause damage to any services not backed up with auxiliary generators, potentially affecting everything from transportation links to desalination plants.

Although energy infrastructure is perhaps the core element of critical national infrastructure (CNI) likely to be targeted by a foreign power, this is not a counsel for despair and certainly not for a "head in the sand" approach. CEOs and CIOs of oil and gas companies should take a systematic approach to surveying and then mitigating cyber risk, which can help insulate them from the worst impacts of an attack, even if total prevention remains an impossibility.

Companies need to understand their risk profile before any mitigation can begin in earnest. This involves understanding their assets, the full range of threats they may face and the vulnerabilities. The first is often one of the hardest for energy companies, which have dispersed assets all the way through their business process, from extraction to refining through to distribution.

Threat assessment is often best done by a third party, be that a national CERT team, or a private sector security consulting firm; these are likely to have a much clearer notion of the national threat picture. Vulnerabilities may arise from a number of different areas including technology, processes and people.

The latter should never be overlooked as a threat, for companies which employ thousands of people, vetting and control systems are vital to prevent either malicious action or incompetence. Once the cyber security function of the company has a firm handle on their risk profile they can then move to take appropriate mitigation measures.

Mitigating the cyber risks can be looked at across three broad areas Visibility, Intelligence and Integration.

Visibility means truly understanding what is on your environment, who is on your environment and how is your environment configuration. Knowing these things and continually monitoring them for vulnerabilities and insecurities allows companies to continuously remediate and mitigate cyber risks. Large companies in particular, often maintain networks patched together over decades, running different generations of hardware and software. It's a simple truth that you can't protect what you don't understand; a thorough audit is vital at the start of any mitigation process. Developing and maintaining the capability to performing this auditing on a continuous basis will increase your security posture and allow for the window of vulnerability to shrink in duration.

Intelligence relates your understanding of the ever changing threat landscape and the constant discovery of vulnerabilities within ICT systems. There is no single source of cyber threat intelligence or vulnerability information so a program needs to be established to identify and capture the most appropriate sources for your organisation. This could include open sources, academic and research institutes, government agencies, commercial feeds, and industry

information sharing programs. Intelligence also includes having a clear understanding of the critical information necessary for your particular line of business.

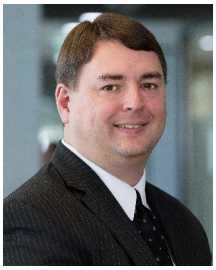
Integration aggregates the information found in the other two phases, and displays them in a format which can be readily understood by decision makers to enable them to act quickly. In particular, attacks should be logged and diagnosed in a systematic fashion.

Energy firms armed with this complete picture should then be able to create a continuous monitoring and mitigation capability supported by intelligence and securely integrated technology. As programs mature a well-integrated capability will facilitate advanced mitigation strategies that leverage machine learning and security automation to accelerate remediation and mitigation actions.

It's going to be a challenging time ahead, but with the right planning, commitment to innovation and sensible practices, nations and companies can mitigate, if not completely prevent, cyber security attacks.

It's the responsibility of both the private and public sectors working hand-in-hand to ensure infrastructure as vital as oil and gas platforms is not just defended from physical attack, but shielded from the predations of hostile states and criminals. To ignore the threat is to leave your nation hostage to the next malware attack.

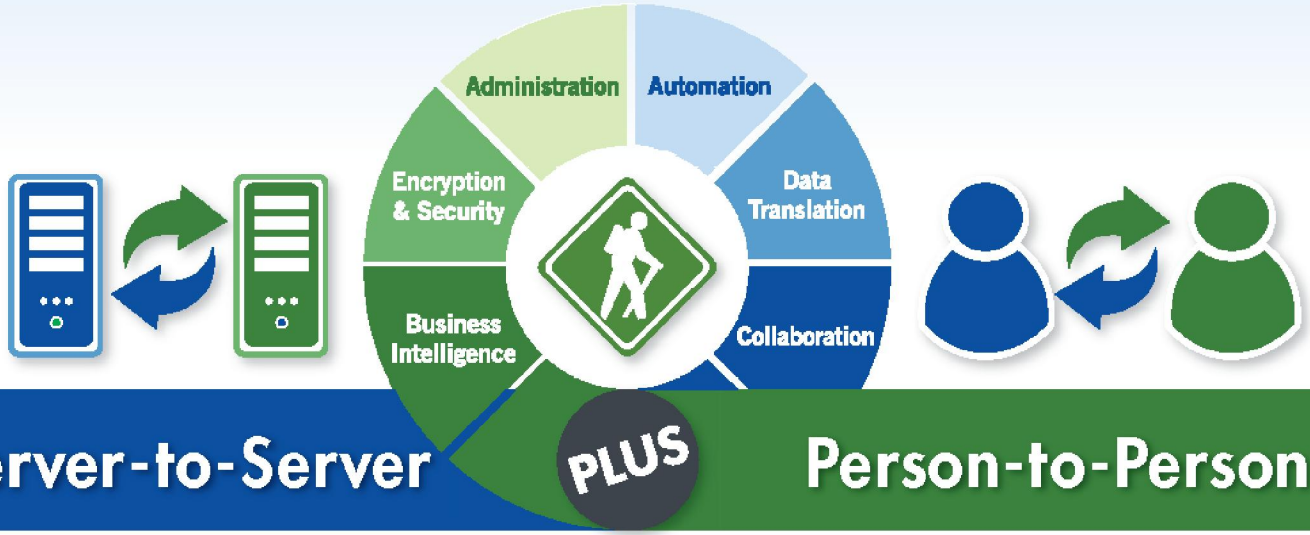
About the Author



Eric Eifert is the Senior Vice President of Managed Security Services at DarkMatter. With more than 20 years of military and civilian experience in information technology and cyber security, Eric leads the DarkMatter team of security and technology professionals. His team provides customers onsite and remote security operations centre services. These include intrusion detection and prevention, security event monitoring and detection, incident investigation, 24/7 continuous diagnostics and mitigation, and event resolution. Eric and his team also assist customers in designing and building insider threat detection capabilities; integrated network and security operation centres; continuous governance, risk and compliance monitoring; and cyber-situational awareness dashboards.

Prior to joining DarkMatter in 2015, Eric was Senior Vice President of the Cyber Security Solutions Division within US-headquartered ManTech's Mission Cyber and Intelligence Solutions Group. He led a highly technical team of more than 450 cyber security experts in the provision of a range of solutions for federal and state governments, and commercial and international customers. Eric also is an adjunct professor in the Department of Electrical and Computer Engineering at George Mason University, Virginia, U.S., teaching graduate digital forensics analysis and cyber investigations. Prior to and concurrent with his role at ManTech, Eric spent 20 years with the U.S. Air Force Office of Investigations in positions such as Network Engineer, Special Agent, Computer Crime Investigator, and Commander.

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

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

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

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

Visit GoAnywhere.com for a FREE trial.

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

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

One of the Largest North American Railroads

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

GoAnywhere.com 800.949.4696

"Best Overall Value" and "Leader" awards -- Info-Tech Research Group, Managed File Transfer Vendor Landscape Review 2015

The Challenges and Opportunities of Building a Unique and Memorable Cybersecurity Brand

By Evan Goldberg, director, AR|PR

As the dust settles from the 25th Annual RSA Conference, attendees with roots tracing back to cybersecurity's early days were again reminded of the event's evolution from its origins as a simple "forum for cryptographers to gather and share the latest knowledge and advancements in the area of Internet security," into a global tradeshow akin to the biggest of any industry. This year, more than 500 companies exhibited their products and services in addition to the numerous panel discussions, dozens of training sessions and high profile keynote speakers that participated throughout the week.

Despite RSA's popularity, many of the industry's most seasoned veterans have begun to voice concerns over the lack of both perceived and actual competitive differentiation among the roster of cybersecurity vendors that the show attracts each year. As KPCB's Ted Schlein told Venturebeat in December 2015, "With the growth in the number of companies in this field (cybersecurity), a lot of them start to sound the same." More than $7.6 billion has been invested in hundreds of cybersecurity companies since 2013.

From endpoint security, anomaly detection and email security to identity management, situational awareness and anti-virus; to application security, cloud security, data security and virtualization, there is no shortage in distinction of cybersecurity products and services. Yet, , many industry leaders, such as Mahendra Ramsinghani, the founder of Secure Octane, a cybersecurity seed fund, argue that product differentiation isn't projecting into unique brand identity. As Ramsinghani told Techcrunch, "the security bazaar is noisier and messier than ever. Every company sounds exactly like the eight others, and lines get blurred. Those that thrive will do so on differentiation."

With opportunity abound (Gartner projects the cybersecurity industry to surpass $170 billion worldwide by 2020), why do so many cybersecurity companies either struggle to build or devalue the importance of creating strong and memorable brand identities?

Unique Challenges of Building a Cybersecurity Brand

While cybersecurity companies would be well suited to pursue some of the brand building strategies that help companies in other industries thrive, there are some unique challenges that complicate efforts. These include:

1. **Distrust of Marketers** – Cybersecurity entrepreneurs don't always see eye-to-eye with marketing, especially in early stages in which engineers and developers are highly engaged in brand development.

2. **Difficult to Tell Customer Stories** – Most companies do not reveal details of attempted or successful cyber attacks. As such, it's infinitely more complex to validate products and services, as marketers don't have success stories to tell.

3. **Subject Matter is Inherently Fearful** – Branding to FUD (fear, uncertainty and doubt) has become the default strategy for most cybersecurity companies, limiting opportunities for competitive differentiation.

4. **Education Gap Between Companies and Customers** - Very few companies have more than a person or two that speaks the language of cybersecurity, challenging how marketers can showcase value and potential ROI.

5. **Competition Requires Expedience to Market** – $3.8 billion dollars was invested in cybersecurity companies in 2015, according to CB Insights. With funding breads competition and with competition requires an accelerated time to market. In doing so, the best practices of brand building are often ignored or pushed to the side.

6. **Perception of Highly Confidential Intellectual Property** – Cybersecurity pros are known for being paranoid about IP theft or product replication until patents are secured. As such, constraints, sometimes significant, are placed on marketers to ensure confidentiality.

10 Tips for Building a Cybersecurity Brand

Although challenges to building cyber brands exist, there are some companies, like AlienVault, Digital Guardian, and Cylance, which have built memorable brands. For startups and growth stage cyber companies in need of establishing or refining their brand, here are 10 tips to consider.

1. **Don't Devalue Messaging**– Messaging is one of the most important tactics of brand building. Companies must effectively, consistently and concisely talk to value proposition, key differentiators, and reasons to believe using language that resonates among the different personas of the target audiences.

2. **Website Should Engage First, Educate Second** – Avoid too much industry jargon, overtly technical language or FUD on the homepage, as you have less than 10 seconds to connect with website visitors before they leave your site for good.

3. **Visual Identity Matters** – 65% of people are visual learners, meaning your brand's visual identify must convey the virtues of the value proposition. Recognize that some revenue may be tied to visual engagement.

4. **Fear the Overuse of "Fear" –** Don't let your brand become synonymous with FUD. Differentiate by striking balance in the tone and style of your messaging and visual identity. Endpoint Security Company Barkly does a good job of keeping things positive.

5. **Don't Hide from Media –** Even if your product requires "stealth," there are plenty of opportunities to begin building awareness and perception. Write a contributed article for an industry trade or place commentary inside of news stories. Cyber Defense Magazine is very accepting of vendor-neutral contributions every month.

6. **Embrace Content Diversity –** Effective content comes in many different forms and is syndicated via many different channels. From customer playbooks and use cases to infographics, Vine videos and, of course, whitepapers, the opportunities available to your brand are endless.

7. **Digital Breeds ROI** – Discrediting digital and social media is outdated and detrimental to building brands – even in cybersecurity. Today, Tweets actually boost SEO, and 90 percent of journalists are on Linkedin. Furthermore, studies show that buyers, whether B2B or B2C, view a company's social presence as a commitment to the consumer.

8. **Trust Your Marketing Team –** Essential to the development of any cyber brand is the company's trust and support of its marketing team. Even if that team consists of just one person, empower him or her with the tools and resources that they need to thrive.

9. **Marketing Automation is Your Friend –** There are many tools available to help businesses automate marketing processes. Invest early and often in programs like Hubspot, Automational, or Sprout Social to help nurture leads and drive customer engagement and satisfaction.

10. **Try Something New Once Per Quarter –** Whether it's a $50 sponsored ad on Linkedin, a short-term Google ad words campaign, or developing an infographic, try something new each quarter. Don't forget what its like to not be afraid to fail in the face of the unknown.

Building a brand isn't easy, but its especially challenging for cybersecurity companies in the midst of a supremely competitive and swiftly growing market. But that doesn't mean it cannot be done, as long as its importance is both embraced and prioritized.

About the Author

Evan Goldberg is a director at AR|PR and the agency's media and messaging guru. He is also the lead of the cybersecurity practice group.

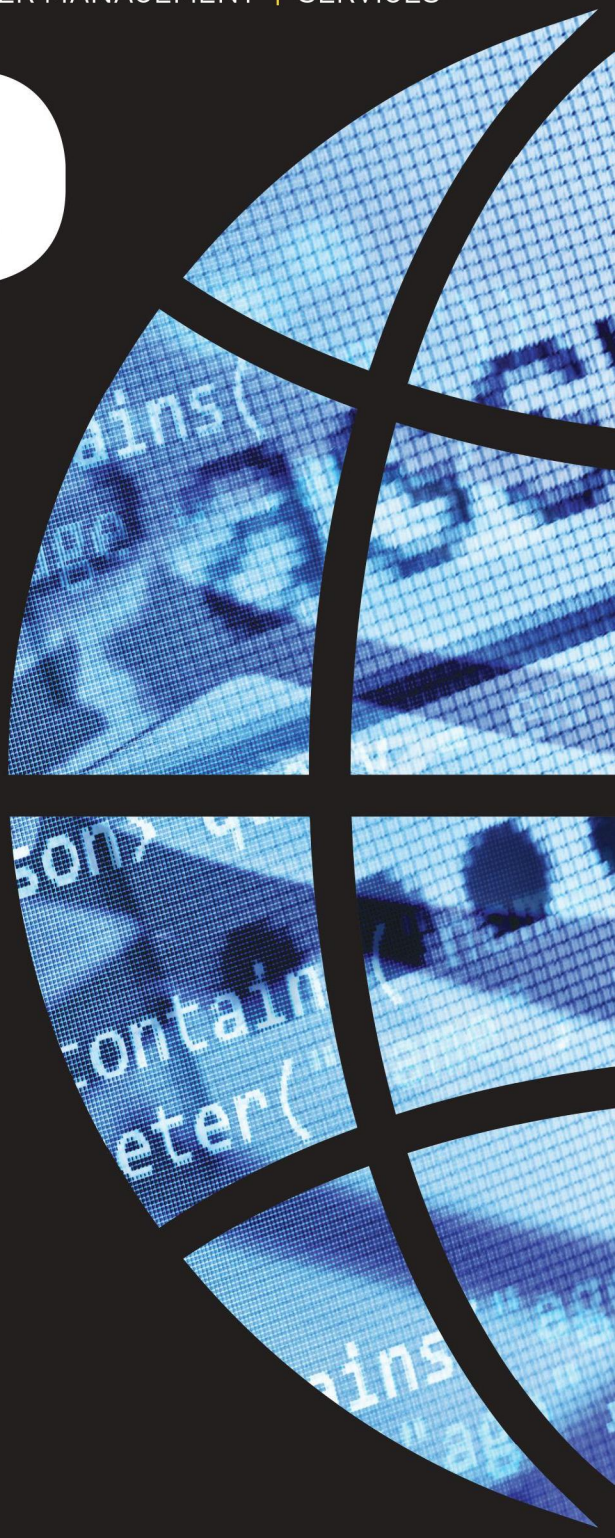
CNI PROTECTION | CYBER SECURITY | POLICING AND LAW ENFORCEMENT
MAJOR EVENT SECURITY | BORDER SECURITY | OFFENDER MANAGEMENT | SERVICES

SECURITY & COUNTER TERROR EXPO

19-20 APRIL 2016 | OLYMPIA LONDON

Supported by

Home Office



The leading event for public and private sector security and counter terror professionals

Free-to-attend Cyber Threat Intelligence Conference

- Insight into global cyber security threats from internationally recognised experts
- Discover the increasingly sophisticated technology used by cyber criminals
- Learn best practice techniques in mitigating cyber attacks

Cyber Threat Intelligence brings together all those who must prevent or prepare for cyber terrorism or cyber-crime.

Presented by: techUK

#SCTX16

Register as a free visitor online and save £50

www.counterterrorexpo.com/cyberdefense

Co-located with: FORENSICS EUROPE EXPO; Ambition The EPRR Expo

Sponsored by: MEESONS SAFE SECURE ACCESS; xtralis The sooner you know

Follow us on

Organised by: CLARION EVENTS

FERC's Delaying of NERC CIP V5 Implementation Reinforces Need for Strong Cybersecurity Culture

By Doug Wylie, CISSP

Last week, the Federal Energy Regulatory Commission (FERC) granted a motion to postpone implementation of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) V5 Standards from April until July 1, 2016. Ted Gutierrez, the industrial control systems (ICS) & NERC CIP Product Manager at the SANS Institute conceded that the announcement was indeed, "a head scratching move from FERC," as the implementation of V5 is now delayed to coincide with the unveiling of V6 standards. As such, facility owners and operators may choose to disregard V5 implementation, despite financial penalty, and opt instead to prepare for the V6 standards.

In November 2013, FERC approved Version 5 of NERC CIP and the requirements for which owners and operators were to conform was supposed to become enforceable beginning in April of 2016. Version 5 represents the most material change in requirements in more than 10 years, which is demonstrative of both the expanding threat landscape, and the progress achieved in mitigating cyber risks to the electric grid. Most notably, penalties for noncompliance can include a fine of up to $1 million per day per violation.

The NERC CIP V5 standards incorporate a significantly larger scope of the systems protected, and all facilities that meet the definition of bulk electric system (BES) will now be subject to the regulations. This part of the mandate, in particular, represents a major step forward in securing the integrity of American power and utilities, and is especially important following confirmation that a malware attack crippled the Ukrainian power grid and reports that Japan's critical infrastructure is under repeated attack.

The current CIP standards, Version 3, only comprise power facilities determined to be critical assets by their owner or operators. Because of this optionality and difficulty in determination, many facilities chose not to position themselves as critical, in order to avoid the compliance obligations. With Version 5, however, every BES facility will be subject to at least some requirements.

One of the primary additions to NERC CIP V5 is the demand of BES facilities to continuously monitor their network communications, which is something that our Sophia product can help with. NERC CIP V5 also mandates systems to have one or more methods for detecting malicious communications, such as an intrusion detection system or application layer firewall. Methods of threat detection to deter, detect and prevent systems penetration from malware, attack scripts, and exploit framework, are required by NERC CIP V5, as well. In addition to more proactive detection and mitigation of threats, facility owners and operators will also be required to log cybersecurity incidents from the initial identification, to remediation and all the way through the post-event investigation.

For almost 3 years, NERC has taken a flexible compliance monitoring and enforcement approach during what it called a "Transition Period." The goal here was to help with logistical transition, but also to educate owners and operators on the technical security requirements of NERC CIP V5. But with roughly 5 weeks until NERC CIP V5 was set to become enforceable, FERC decided to grant the petition by several electric trade organizations to postpone implementation.

This delay comes as a surprise to many in the industry who have worked so hard over the past three years to reach compliance. As Gutierrez wrote on the SANS blog:

> *"I'm concerned about the perception these types of decisions create. The electric industry is full of hard working, incredibly dedicated people who want to do the right thing. But that thing keeps changing. These folks will undoubtedly feel silly having to explain to their leadership how the race to April 1 wasn't so urgent after all. Frankly it makes FERC, NERC and the industry look inept to those not close enough to understand it all. I really wish the regulators would get their act together and stop putting entities in this position. CIP really is hard enough already."*

While most agree that NERC CIP V5 will help reduce risk, there should be no mistaking the standards as a final or 'absolute' solution in which the majority of cyber risk will be permanently minimized. In fact, the unintended consequence of any regulation is that it can still easily lead organizations into a 'check-the-box' mentality. Instead, standards should be interpreted as models and guides for industries and organizations to take action rather than sit idle to admire new and existing security challenges and threats.

Only time will tell how seriously owners and operators take V5 now that V6 is confirmed to release on the same day that V5 is scheduled to take effect. Regardless, this delay underscores the need for the energy industry to create a security culture that prioritizes the mitigation of dangerous and frequent cyber threats over the politics that hinder even the most well intentioned industry standards and guidelines.

About the Author

Doug Wylie is the vice president of product marketing at NexDefense, a leading provider of cybersecurity for industrial control systems.

Why Cybersecurity Training Isn't Just for IT Professionals

By Marc Saldana, Cyber Defense Solutions LLC

As the realm of cybersecurity continues to evolve at a rapid pace, industry leaders are constantly challenged to stay ahead of cyber threats. Cybercrime, cyber espionage and cyber terrorism by nations, criminal groups and script-kiddies are at record-high levels, and show no sign of decreasing any time soon.

As cyber threats posed against government agencies, industry, internet-connected infrastructure and personal data grow, so does the need for highly-trained cybersecurity professionals and trained employees across all levels.

In a new era of social and online activity, cybersecurity training has seen tremendous growth. Why? Because it takes an arsenal of skilled professionals at every level of an organization to protect sensitive data. Cybersecurity training and certification are key to understanding the ever-changing threat landscape, staying ahead of the technology curve and learning how to quickly detect and mitigate threats.

Cybersecurity Training for All Employees, at All Levels

Many organizations believe that cybersecurity training is only valuable to those tasked with protecting the network. However, cybersecurity training for all employees—from the mail room to the boardroom—is essential. Year after year, the loss of proprietary company technical data and classified government information continues to increase, mainly because people are the weakest link in cybersecurity.

Unknowingly, employees can cause the greatest damage to a network. Cybersecurity training educates employees against threats such as clicking on links within phishing emails, visiting suspect websites and downloading or installing non-approved software that can compromise a network and data.

While phishing scams have been around for years, they have become quite sophisticated and hard to detect. In fact, clicking on phishing emails continues to be the number one way networks are infected, data is stolen and network equipment (computers, laptops, servers, etc.) are damaged. Training employees on the warning signs of a phishing scam, even if the email appears to be from a trusted source, can help to prevent real damage and exposure of sensitive data.

While the case for basic cybersecurity training for all levels of employees in an organization is self-evident, often times, "C" level executive training is a low priority. However, executives are some of the biggest targets of advanced cyber threat actors. All too often, CEOs, CISOs and COOs do not truly understand the real risks and vulnerabilities posed against their data, networks and computing resources from the most experienced threat actors.

The need for “C” level understanding and leadership is vital in defending against the threat. Executive-level training should include all of the basic training required for the entire workforce of the organization; some mid-level awareness training in order to understand the true nature of the threat; and, at a senior-level, knowledge of network vulnerabilities and the risk management required to assist in the tough decisions necessary in the delicate balance of budget spending for IT security and training that is necessary to mitigate threats.

Training and Certification for the Cybersecurity Professional

While there is no “silver bullet” to protect against all cyber threats, there are advanced training and certificate programs that help cybersecurity professionals develop their expertise. From the novice to the seasoned professional, the cybersecurity field offers a vast selection of career opportunities and areas of specialization, each with specific training and certification requirements.

For those entering or in the early stages of a cybersecurity career, training and certifications provide an advantage over the competition to “get their foot in the door” of a IT security position, especially as the gap between the number of trained cybersecurity professionals and the need for such workers continues to grow. Security-related certifications are a requirement for cybersecurity jobs in the government as well as most industry positions.

With rampant resume inflation and degrees that sometimes aren't in technical fields, certifications provide a means to measure knowledge and level of expertise in a given technical field. In addition, certifications are an indicator of expertise in both written knowledge and in operating essential types of Computer Network Defense (CND) specific tools. General IT certifications such as those available at the myriad of training companies assist in providing the essential skills for network security and risk management, all of which are often the foundation for a career in cybersecurity.

On-going training and certifications help cyber security professionals broaden their skill-sets and are the discriminators for career advancement into management positions and the higher end of the pay scale. For the seasoned cybersecurity professional, training provides the opportunity to gain the technical knowledge necessary to hunt for and remove malicious files, create signatures to detect and protect from future similar events, create procedures to assist with preventing similar future threats, and help assign attribution to the entity that caused the threat.

Examples of advanced certifications include the Certified Information Systems Security Professional (CISSP), the Certified Penetration Testing Consultant (CPTC), the GIAC Certified Penetration Tester (GPEN), the Offensive Security Certified Professional (OSCP), the Certified Ethical Hacker (CEH), the EC-Council Certified Security Analyst (ECSA) and the GIAC Reverse Engineering Malware (GREM).

These advanced certifications among many others enable cyber personnel to manage day-to-day job challenges in a demanding threat environment.

With each passing year, more and more negative publicity is given to significant cybersecurity incidents. Last year's Office of Personnel Management's (OPM) data breach had far reaching impact, putting millions of government and contract worker's personal data at risk. In order to detect, protect and mitigate real cyber threats such as the insider threat, identity theft, spyware, malicious code and phishing, it's important to have a culture of cyber threat awareness engrained in every employee within an organization, especially government agencies. Achieving optimal performance in day-to-day operations while managing ever-evolving threats and responding to incidents is an ongoing challenge. Investing in cybersecurity training provides the skills needed to keep up with—and get ahead of—cyber threats.

About the Author

Marc Saldana brings more than 28 years of experience supporting the Department of Defense (DoD) and the Intelligence Community (IC) as both a member of the U.S. Navy and a government contractor. His deep and varied professional background includes positions such as Cryptologic Technician, Sr. Security Analyst, Computer Network Defense Engineer, Computer Network Defense Service Provider (CNDSP) SME, Lead Technical Trainer, Network Defense Watch Officer, Information Systems Security Manager (ISSM) and others. Marc is a service-disabled veteran who served 14 years in the U.S. Navy.

His military assignments included diverse roles such as Leading Petty Officer, Information Security System Manager, and Certified Instructor. As a civilian, his experience and background have led him to opportunities supporting operations at distinct, globally-dispersed teams providing critical information technology services to various client organizations, including the Join Task Force-Global Network Operations (JTF-GNO), Counterintelligence Field Activity (CIFA) and currently, Cyber Defense Solutions, LLC. Marc has a degree in Technical Studies (Computer Technologies). He has a CISSP and is certified by the U.S. Navy as an Instructor and Information Systems Security Manager.

About CDS

Cyber Defense Solutions LLC (CDS) is a full-service information technology (IT) company known for cutting-edge cyber security solutions that tackle the most complex tasks. As a Service-Disabled Veteran-Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), and Minority-Owned Business (MOB), CDS is committed to providing government customers with flexible technology solutions and services for today's complex cyber threat landscape. CDS' Cyber Training Institute provides timely access to essential, blended training to improve workforce development and mission success. To learn more, visit www.cyberds.com.

Combating Human Error on an Organizational Level

The transition to an economy more reliant upon services and technology means that more private information and business data will be available for hackers to steal, requiring a deeper commitment to cybersecurity from all interested parties. There are billions to trillions of dollars of property at stake overall. This creates a natural incentive for hackers and cybercriminal activity that target corporations and business leaders.

Unfortunately, many decision makers are given to thinking that the latest and greatest firewalls and security tools are all that are needed in order to protect these vital assets. They spend thousands on some programs, tell their IT departments to do what's best, and go about their business. This is the kind of thinking that leads to the economic and reputational ruin of a data breach.

The best tools are indeed absolutely necessary, but they need to be used in conjunction with a cybersecurity strategy that is as thorough as it is adaptive in combating the dangers of human error. A company's cybersecurity infrastructure is only as strong as its weakest link, and most of the time, it is employees who work with data and still do things such as use "password" as a verification measure. It could be the subject of humor if it weren't real. Cybersecurity professionals need to have a response to this problem.

Here are the trends that every cybersecurity professional needs to know about:

Training Is Not Universal

Cybersecurity isn't often taught in school, and with most societies the most that you can expect is a couple of (poorly advertised) websites with tips and a government department woefully underequipped to tackle the problems at hand. This leads to the law of the jungle being the law of the online landscape. Training should never be assumed when managing new hires or existing employees who will work with vital information.

There are IT professionals to handle the large-scale problems and exploits, but the human problems cannot be tackled solely by technological measures. Some restrictions such as web filtering software could be used, but it could undermine the goals of the organization while still leaving blatant offenses as a risk.

Consider the following as training options to reduce risk:

- A method of evaluation and testing so that managers can know who needs further training and to what extent that training is necessary. Teaching the absolute basics to someone who knows their way around the internet can be seen as condescending to the employee and a waste of time.
- Training on certain technology topics becomes obsolete over time. While some things such as password use and device security remain constant, the specifics of which security tools to use and new types of scams that pop up require additional periodic training.
- Keep a policy open that if there are any questions regarding cybersecurity of scamming topics that there is a designated person who will happily answer them. Encourage erring on the side of caution. Don't penalize people who ask something that seems obvious. Dozens of simple questions are worth one that prevents a human error related data breach.

Training Is Often Inadequate

While the above strategies are great ways to handle training timelines and objectives, many companies that already include measures such as those don't go far enough with the specifics of what they teach. For a basic example, memos go out proclaiming the importance of verification measures, but those same memos don't give examples of what the best passwords or security question answers may be. Cybersecurity professionals need to recognize these gaps and fill in information when needed.

Here are a few areas which are often found sorely lacking:

- Cloud services are commonly used by people, but they are one of the most problematic areas for cybersecurity professionals. Misinformed sharing choices often lead to leaked files, and managers often assume that people know how to use these services. Proper training regarding an organization's cloud service of choice can lead to increased efficiency and precise knowledge of who files go to and stay with once the "share" button is pressed.
- Smartphones are effectively small computers that are often underestimated in how important they are to a company's technology infrastructure. Too many important

messages are sent and received over them for related security training to be ignored, and as such, training procedures specifically focusing on them are recommended for any individual. Each OS has its own security tools available for use, and data management on smartphones is a woefully neglected skill.

- While this an extremely complex skill if looked at too deeply, anyone working with data should be taught the basics of computer networking and the different protocols and options used. Knowing the importance of keeping a network private or keeping a firewall turned on will motivate people to keep those very habits.

Environments and Device Policies Make a Difference

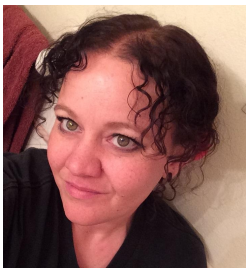
Networks are not created equal from a cybersecurity standpoint, and businesses and individuals alike need to realize that the public network hosted by your local café is a shark tank of hackers hoping to intercept data on public networks. If employees meet clients in these locations or work while they travel they need to learn to use of Virtual Private Networks (VPN) so that they can protect themselves and the data under their jurisdiction. They similarly need to get a VPN that is of a high quality so any doubt can be left behind as to their level of protection.

Human error also comes about more easily from the mixing of work and personal devices. Checking a social media account is one thing, but too often people of all types will try to be more efficient only to be counterproductive at that task, distracting themselves and leaving their machines open to more risks than necessary. It should be advised as a company policy that these devices should remain separate, even if it means that a company supply the necessary devices themselves.

This is a complex issue that will only grow more complex as more threats emerge and the importance of cybersecurity grows. Companies are starting to feel the need to improve their cybersecurity posture (whether through consequences of law or more general reasoning), and as such they are going to turn to the experts and those with cybersecurity knowledge. Recognize the gaps where you see them and talk to the people that matter.

Share this information with your company and/or clients so that the world becomes a safer place. Whether you like it or not, people with data to keep safe have to rely on larger structures and organizations to pull their weight. Keep the discussion going, and be bold in your efforts to make people more conscious of their cybersecurity problems.

About the Author



Jen Martinson is an internet security specialist and editor-in-chief for Secure Thoughts, an excellent resource for important internet security information. She loves to share her security tips with other users and has set out to make the internet a safer place for all!

sponsors

simplivity box CYLANCE zscaler

Join the top IT Leaders from Texas, Oklahoma, Louisiana and Arkansas as they discuss regional IT challenges facing the region. IT service providers and executives will engage through presentations on top industry trends, one-on-one engagements and open-discussion group meetings.

Topics include:

- Redefining the IT Strategy for the "New" Enterprise
- The Changing Role of Outsourcing
- The Platformization of IT -A Digital Transformation Journey

CSA cloud security alliance℠

Cloud Security Panel -
Hosted by Cloud Security Alliance

Confirmed Attendees

CSA cloud security alliance℠ | CLUBCORP | GE Oil & Gas | CBRE

To learn more about sponsoring or attending the *SINC TOLA IT Leaders Forum* please email info@sincusa.com.

408.465.2727 | SINCUSA.COM | INFO@SINCUSA.COM

Cyber Risk: The Nitty Gritty on Today's Threat Landscape

Known Vulnerabilities and Increasing Sophistication of Adversaries Place Organizations at Risk

by Dustin Childs, Senior Security Content Developer, HPE Security Research at Hewlett Packard Enterprise

The security threat landscape continues to evolve as attackers advance their techniques, shift their targets from the perimeter to applications, and increasingly focus on the monetary gain of malware. At the same time, enterprises are still not patching existing vulnerabilities with enough prowess to prevent easy entry points for adversaries. The annual HPE Cyber Risk Report provides detailed insight into the changing threat and vulnerability landscape, as well as how enterprises must meet both exisiting and new challenges. Here are a few of the key themes from the report.

1. **We learned nothing about patching**

One item that stands out in the current report is the most successfully exploited vulnerability in 2015. The number one exploit now clocks in at five years old – and it was 2014's number one exploit as well. This is despite the vulnerability, a Stuxnet infection vector (CVE-2010-2568), having received two separate patches from the vendor. This is especially concerning as attackers will typically focus on known vulnerabilities first, since they provide the easiest entry point. Applying patches in an enterprise is not as simple as it seems, and can be complex and costly – especially when problems occur. While the past year saw a record number of patches from both Microsoft and Adobe, they do little good if they are not installed by the end user. The most common explanation given by those who disable automatic updates or fail to install patches is that they break things. Vendors must do more to reestablish the trust in patches. Without this trust, enterprises will remain wary of installing patches out of a fear of what might break.

While installing point-fix patches remains vital in protecting users and networks, it also might not be sustainable at current volumes. However, one positive trend is the shift from point-fixes to broad impact solutions. Instead of releasing patches to fix many different vulnerabilities, these defensive measures take out an entire class of attacks – at least for some period of time. For example, the past year saw the inclusion of use-after-free protections in Microsoft browsers Internet Explorer and Edge, which provided wide-reaching fixes to disrupt attacks in an asymmetric fashion. Other vendors would do well to consider implementing similar strategies to disrupt classes of attacks. The attack surface reduction provided by patching and other security-related fixes can be far reaching.

2. **The monetization of malware**

Just as the marketplace grows for vulnerabilities, malware in 2015 took on a new focus. In today's world, malware needs to produce revenue, not just be disruptive. This has led to an

increase in ATM-related malware, banking Trojans, and ransomware. The report found that more than 100,000 banking Trojans were detected in 2015 alone.

However, malware rarely uses new or undiscovered vulnerabilities. Instead, most malware relies on bugs previously fixed by the vendor, but not widely remediated in an enterprise, which reinforces the importance of installing patches and updating software.

3. **Attackers have shifted their efforts to directly attack applications**

As attackers continue to evolve their methods, defenders must recognize their enterprises are evolving as well. The traditional network perimeter has dissolved, and with today's mobile devices and broad interconnectivity, the actual network perimeter is likely in someone's pocket right now. According to the report, approximately 75 percent of the mobile applications scanned exhibited at least one critical or high-severity security vulnerability. Attackers realize this too, and are no longer just targeting servers and operating systems. They have shifted to directly targeting these applications. Attackers see this as the easiest route to data held within an enterprise and are doing everything they can to exploit it.

Today's security practitioner must understand the risk of convenience and interconnectivity to adequately protect it. They must build security into every facet of the IT stack and focus on protecting the interactions between users, apps and data regardless of device or location.

Combating the changing threat landscape

Just as the report shows the means by which attackers evolve, organizations must shift their focus to meet the threats head on. This evolution might not always be easy or even welcome, but it must occur. Reviewing the Cyber Risk Report 2016 can be that first step taken to better understand the threat landscape, and where to best deploy resources to improve your security posture.

About The Author

Dustin Childs is a senior security content developer and evangelist with Hewlett Packard Enterprise Security Research. In this role, Childs writes and edits security analysis and supporting content from various HPE researchers. Mr. Childs also is responsible for providing insight into the threat landscape, competitive intelligence to the research team, and guidance on the social media roadmap. Mr. Childs focuses much of his research on the practicalities of maintaining security and privacy in the real world through practical solutions, such as patch management. Part of his role also includes speaking publicly and promoting the research and technology of HPE. He has presented at numerous conferences including BlueHat and ThotCon.

Prior to joining HP, Mr. Childs worked in response communications as a part of the Microsoft Trustworthy Computing (TwC) initiative. He also worked as a security program manager in the Microsoft Security Response Center (MSRC) and is a veteran of the U.S. Air Force.

Industry Addresses Challenges in Creating a Cybersecurity-Capable Workforce

By Bob Chaput, CEO & Founder, Clearwater Compliance

Today there are an estimated one million job openings in the cybersecurity industry, according to a Cisco report. That figure is expected to jump to 1.5 million unfilled positions by 2019.

Dice, a career website serving information technology and engineering professionals, recently reported a 90% year-over-year increase in cybersecurity jobs. Based on these figures, it appears the industry is heading in the wrong direction; demand for cybersecurity skills is on the rise, and filling positions can be a long and difficult process, according to Search Security.

What's more, job postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program. A recent survey by IDC and T.E.N. said it takes an estimated three months to fill cybersecurity job openings — while senior leadership positions can take well over 12 months.

This industry-wide employee shortage is creating significant challenges inside the walls of today's companies — problems compounded by the rising number and severity of security breaches. According to a 451 Research study, 34.5% of security managers reported significant obstacles in implementing security projects due to lack of staff expertise. As a result, only 24% of enterprises have 24×7 monitoring in place using internal resources.

That's the bad news. The good news that is a career in info-security is considered one of the smartest choices available today — and for the next seven years. U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015.

It's not just a skills issue within the organization. To date, publicly traded companies have not been required to nominate directors who are cybersecurity experts. Legislation recently introduced by Senators Jack Reed (D-RI) and Susan Collins (R-ME) aims to embrace Commissioner Aguilar's suggestion. The Cybersecurity Disclosure Act of 2015 (S.2410) would require the SEC to issue rules requiring public companies to disclose in their annual reports or proxy statements whether any members of a company's board of directors have any expertise or experience in cybersecurity and, if none, to describe what other steps have been taken to address cybersecurity when evaluating potential nominees.

Clearly, this challenge has to be conquered now if our nation's corporate world and government are going to keep their systems safe. The anxiety-producing statistics prove that the cybersecurity industry must do more to attract the nation's best and brightest to this industry and give them the skills needed to succeed.

Finding 1 million-plus new workers won't happen from one single initiative. It's going to take the whole industry — including the government, schools, organizations and companies — to create new pathways to "one of the best jobs out there."

Initiatives Underway to Build a Larger Workforce

There are already several industry, company and organization initiatives underway to attract, train and hire more security professionals. Here is a partial overview of some of the initiatives underway — and leading the way to a larger and stronger workforce.

Industry Collaboration

In April 2014, a dozen leading cybersecurity organizations were invited to convene at RSA Conference 2015 for a first-of-its-kind meeting. The purpose was to begin working toward the establishment of a universal framework for resolving the shortfall of qualified people in the cybersecurity profession.

The group identified some of the contributing factors to this employee shortfall including:

- A disconnect between what skill sets businesses ask for from human resources and what they actually need
- The need for common definitions of job descriptions and responsibilities
- Recognizing the U.S. versus global differences in job definitions and staffing requirements
- The need for all groups within the industry to collaborate to define the profession

Company Initiatives

Symantec is one of several companies working to solve the security worker shortage. In an effort to help fill the job gap, Symantec launched Symantec Cyber Career Connection (SC3) in 2014. The focus of the program, according to CEO Michael Brown, is on training underserved populations like women, youth, people of color, and veterans to help get them to a level where they can get the education, training and certifications they need for cybersecurity jobs. The program addresses four key challenges across the workforce pipeline:

- **Excite.** The program supports non-profits and educators in raising awareness of the long-term career opportunities of cybersecurity.
- **Recruit, train, and certify.** It recruits underserved populations into the field of cybersecurity, and offers industry-recognized training programs implemented through a network of partners.

- **Job preparation.** SC3 places students in cybersecurity internships for on-the-job preparation.
- **Launch careers.** The program connects program graduates to cybersecurity positions through Symantec's network of customers and partners.

Industry Organization Initiatives

In 2014, the Information Systems Security Association (ISSA) launched a program designed to help professionals better understand the various levels of jobs within cybersecurity, so they can better steer their education and training in the right direction. The program, called Cybersecurity Career Lifecycle (CSCL), divides cyber careers into five stages, showing the opportunity for a variety of paths within each level. The levels include:

- **Pre-Professional.** Any individual who has not yet worked in the cybersecurity industry, but may be interested in doing so, such as former military, law enforcement and students.
- **Entry Level.** An individual who has a job in cybersecurity, but has not yet mastered general cybersecurity methodologies and principles, such as associate cybersecurity analysts and cybersecurity risk analysts.
- **Mid-Career.** An individual who has mastered general security methodologies and principles and has determined his or her area of focus, such as cybersecurity forensics analysts and network security engineers.
- **Senior Level.** An individual who has extensive experience in cybersecurity and has been in the profession for 10-plus years, such as senior cybersecurity risk analysts and directors of cybersecurity.
- **Security Leader.** An individual who has extensive security experience, with ability to direct and integrate security into an organization, such as chief information security officers and chief cybersecurity architects.

NIST National Initiative for Cybersecurity Education (NICE)

The National Institute of Standards and Technology (NIST) is leading an educational initiative called the National Initiative for Cybersecurity Education (NICE), which is comprised of 20 federal departments and agencies, academia, and industry organizations. The mission of NICE is to establish an operational, sustainable and continually improving cybersecurity education program to students from kindergarten to post-graduate school. To that end, NICE is working to accelerate the availability of educational and training resources to improve the cyber behavior, skills and knowledge of every segment of the population. To achieve its educational mission, NICE developed three primary goals:

Goal 1 — Accelerate Learning and Skills Development. Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers. Objectives of this goal include stimulating the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers, and engaging displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles.

Goal 2 — Nurture a Diverse Learning Community. Strengthen education and training across the ecosystem to emphasize learning, measure outcomes and diversify the cybersecurity workforce. Objectives of this goal include expanding creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce.

Goal 3 — Guide Career Development and Workforce Planning. Support employers to address market demands and enhance recruitment, hiring, development and retention of cybersecurity talent. Objectives of this goal include developing promotional tools that assist human resource professionals and hiring managers with recruitment, hiring, development and retention of cybersecurity professionals.

These are just some of the steps already underway in an industry dependent on a new, well-educated workforce to accomplish one of the most important challenges of our time — combating an ever-growing number of increasingly damaging internal and external threats.

NIST summed up the challenge in a recent NICE document:

"While billions of dollars are being spent on new technologies to secure the U.S. government (and corporate world) in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success … To effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically skilled and cyber-savvy workforce, and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge."

About The Author

Bob Chaput is the CEO & Founder of Clearwater Compliance. He has 25 years of experience in the Healthcare industry, and his experience includes managing some of the world's largest HR, benefits and healthcare databases, requiring the highest levels of security and privacy. Mr. Chaput continues to expand and update his knowledge base on HIPAA-HITECH compliance through postgraduate study, earning professional certifications and participating in professional healthcare and other organizations.

Bob can be reached online at bob.chaput@clearwatercompliance.com, you can also follow us on twitter @clearwaterHIPAA, and at our company website: https://clearwatercompliance.com

ufi Approved Event

e.oman

Be a part of Oman's only ICT show

.comex

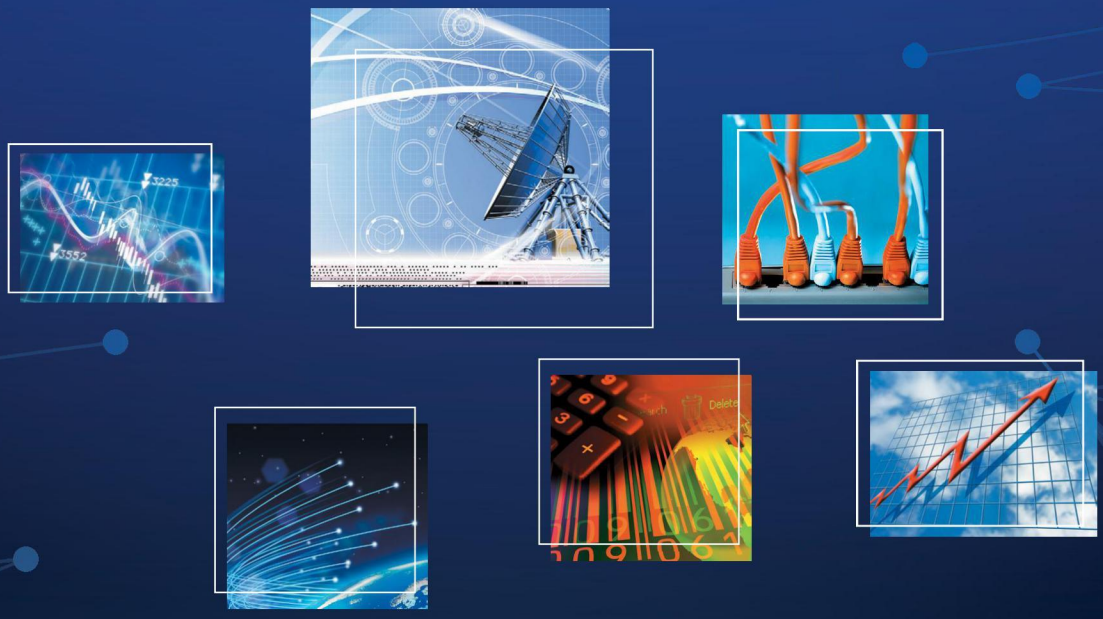
IT, TELECOM & TECHNOLOGY SHOW

26-28 April, 2016

Oman Convention & Exhibition Centre

Muscat - Sultanate of Oman

www.comex.om



For more information on COMEX 2016 Contact

Ashit Barnes
Exhibition Director
+968 9934 1687
barnes@oite.com

Ahmed Farag
Sales Manager
+968 9912 7806
a.farag@oite.com

Research Partners

OXFORD BUSINESS GROUP

Official Magazine

PC

Media Partners

TCM Tech Channel MEA

Telecom Era

Global Security Mag

SECURITY MIDDLE EAST

SSN

Central Asian Cellular Forum

CDM Cyber Defense Magazine

Cyber Security Review

Tedge news.com

Education Technology

DIGITAL FORENSICS / MAGAZINE

Developing Telecoms

Mobilk

Eye Of Dubai

Eye Of Riyadh

Communications Today

Organiser

OITE TRADE FAIRS

www.oite.com

The next generation policing

Today's policing supported with many modern findings about the crime as well as procedures how to resolve the most complicated cases could try to think in advance and suggest some requirements to the new generation police officers which would cope with that standard in the future. If we adopt some good practice nowadays, we could produce the highly capable Police Force tomorrow. Also, it's important to mention that this time's defense system would greatly rely on the emerging equipment and technology, so some skills in that sense would be welcome as well.

First, what would drag someone's attention at the first glance are a behavior and attitude as well as physical shape, so it could be so significant to seek from the police officer to care about those first-sight impressions due to that's something which could offer the confidence about the Police to many civilians. Also, it's so important that Police officers get the good communication skills as well as friendly approach to the people, because they should feel them as the community members which purpose is the protect everyone's needs. We plan to illustrate some of the basic attributes that the Police officer of the new generation should have in Table 1. We believe these characteristics could assure us the Smart Policing in the coming times.

Table 1. The Police officer's most important attributes

Attributes / Level	Very Low	Low	Moderate	High	Very High
Behavioral model	The behavior got fully inappropriate	The behavior got somehow inappropriate	The behavior got satisfactory	The behavior got good	The behavior got highly good
Physical condition	No physical shape	Some physical shape	Average physical shape	Good physical shape	Outstanding physical shape
Positive attitude	No attitude	Some attitude	Moderate attitude	Good attitude	Highly good attitude
Communication skills	Poor skill	Some skill	Average skill	Good skills	Exceptional skills
Interpersonal skills	Poor skills	Some skills	Moderate skills	Good skills	Excellent skills

Confidence	No skill	Some skill	Average skill	Good	Outstanding
Analytical skills	Poorly rational	Somehow	Moderate	Good	Excellent
Critical thinking	Poor reasoning	Some reasoning	Moderate reasoning	Good	Great
Law enforcing skills	No understanding	Some understanding	Moderate	Good	Outstanding
Clearness of reporting	Poor quality	Some quality	Average quality	Good quality	Excellent quality
Situation management skills	Not aware of	Somehow aware of	Able to recognize	Good skill	Great skill

We would not talk about psychological abilities as one of the personal attributes the Police staff should have, but rather try to explain how the positive attitude could mean to a public.

In a reality, the Police members may be under heavy personal or business pressure, but they should deal positively demonstrating the good mental health and encouraging approach to every situation or people within their surroundings.

The medical support and care of the Police officers should get provided regularly or as needed. Even the fundamental requirements to the Police members of the future would seek from them to think, act and resolve the tasks smartly.

The focus of the modern policing should be on a good intellectual development of all staffs getting obtained through education, trainings and most importantly practice and constant improvements.

The qualitative communication is so important to the good information exchange amongst the Police Force members including the well-explained and precisely defined oral statements which could get questionized or even challenged in order to get obtained the best possible information with the perfect timing.

Sometimes it's quite trickery to quantify someone's effort dealing with his professional requirements. Here, we would attempt to explain how the Police staffs' work could get graded.

For instance, the experienced Police members being capable to make a decision based on many practical contributions and results should try to quantify someone's effort as well as support their staffs if they show any sort of struggling.

Today's human society would not deal with the bosses, but rather with leaders being able to pull the other people as well as brightly resolve the most challenging concerns. The Police of tomorrow should cope with these requirements as well.

The new models of policing would deal with the concept of results-driven security, so it's expected that the best players would get ranked the most. The Police are a service created to support their people, while the Police officers should gat well-integrated into their community.

The warm relations between the community members and Police staffs are so significant in sense of good inter-communication offering to the common people to actively participate into their community's lives and activities.

The people love to take part into many social happenings and the Police should offer the chance them to make the changes and get things happen. The community members may realize that their effort could contribute to their own well-being as well as the promising future of the new generations.

It's always good to get a feedback from the people and offer them the system's mechanism which would get trusted and helpful in terms of their needs coordination.

Through this review, we would also mention some critical and analytical skills as well as the level of confidence in sense of dealing with some real-case situations.

The point would be the physical capabilities of the Police members should be at most equally important as their mental performances.

It should get demanded from the Police staffs to get the good

reasoning capacities and always try to support their claims with the good arguments as well as evidence.

Some people may get naturally talented to deal like so, but – in a practice; it's all about well-prepared and conducted trainings and courses which could provide and verify the skills to everyone being capable to serve to the Police Force.

Every Police member must be familiar with the legal regulatory and posses the skill to enforce the law.

Finally, the abilities to manage some situation could get highly important, because non-rarely the inexperienced staffs would not even recognize the situation they are dealing with. For such a reason, it may be significant to conduct the good trainings offering an opportunity to the young officers to get in touch with many different practical scenarios and situations. In other words, the

Police officers would mostly deal as they are trained offering some level of flexibility to the real-case situation.

This contribution would provide an insight into a current situation regarding the policing offering some new ideas how to improve the defense systems seeing the things from a researching perspective.

This set of suggestions would demonstrate some well-researched findings collected from the web, media and publication's resources leaving opened an opportunity to the other researchers as well as defense professionals to use and better develop this update.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia.

She also serves as a Reviewer at the Journal of Computer Sciences and Applications and. She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

ICMC

THE INTERNATIONAL CRISIS MANAGEMENT CONFERENCE

Boston, MA
March 31, 2016

ALOFT BOSTON SEAPORT

The International Crisis Management Conference (ICMC) was created to help support the demand for regionalized education and training for preparedness professionals. The demand for a variety of preparedness skills and a thirst for knowledge with respect to scenario-based training and exercises is at an all-time high. ICMC provides a range of professional speakers that deliver current and interesting topics that are often themed (scenario) based.

www.crisisconferences.com

SPEAKERS:

Keynote Speaker: Leo Taddeo, CSO, Cryptzone

- John McEnness - Exec. Director, Office of Risk Management, RCAB
- Joseph M. Lawless - Director of Maritime Security, Massport
- Mike Lawrence - Chief Reputation Officer, Cone Communications
- Michael Sechrist - VP, Info Technology & Services, State Street
- Jason P. Brennan - Preseident and Co-Founder, Synergy Solutions
- Heather Bearfield - Marcum, LLP
- Robert Burton - Managing Director, PreparedEx, LLC

When you register for ICMC Boston, along with your conference pass, you will also receive:

- **"Introduction to Crisis Simulation Exercises" eLearning Course**
- **Access to digital templates**
- **"5 Steps to Creating and Delivering Tabletop Exercises" eBook**

www.crisisconferences.com

$100 off until February 29th

Register Now!

Limited Seats Available

Our Current Sponsors/Partners

#ICMCBoston

GOLD SPONSORS

CDM CYBER DEFENSE MAGAZINE

PREPAREDEX

SILVER SPONSOR

ICM INSTITUTE FOR CRISIS MANAGEMENT

PARTNERS

Business Continuity Institute

CR JOURNAL

Drupal Security Measures

Drupal is a very popular Content Management System (CMS) on the Internet today. Drupal sites, especially ones running older versions of the CMS or it's modules are a ripe target for attackers.

In this post, we've taken some time to detail a few measures which can be taken to address the basic security holes or malpractices that are commonly present in thousands of Drupal sites.

Running the Latest Version of Drupal

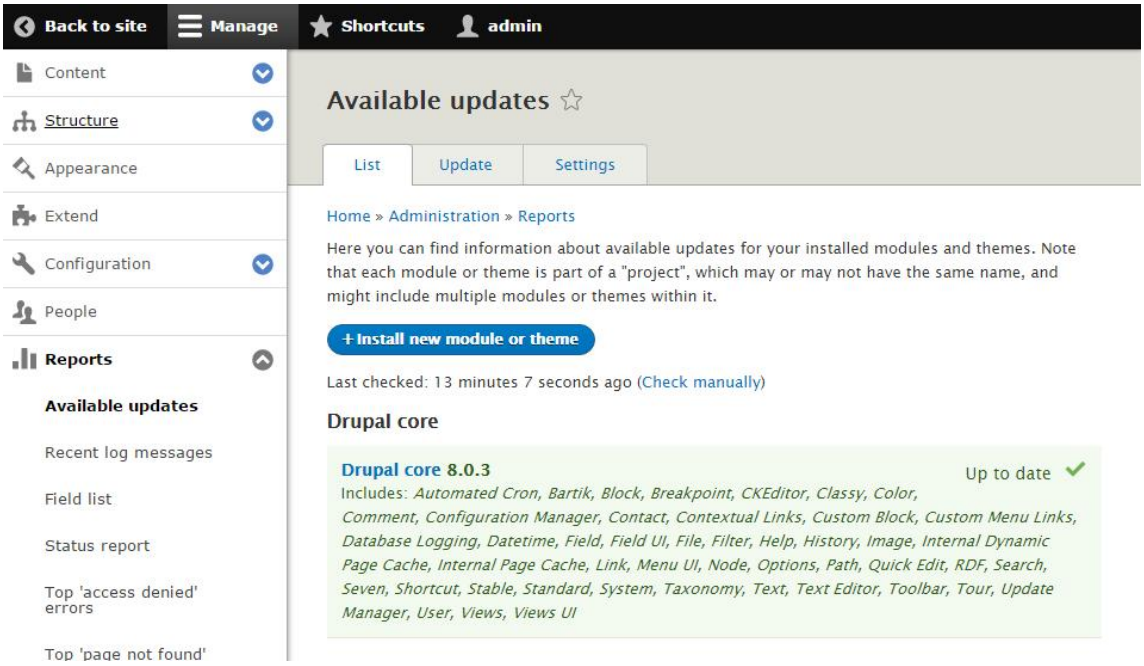
Running the latest version of any software is probably the most obvious first security measure to take. However, with millions of sites still running old and vulnerable versions of the CMS, this point is still one that needs to be stressed.

Updates of Drupal not only bring with them new features, but more importantly, bugfixes and security fixes are made available. Updates help your site remain safe against common, easy-to-exploit vulnerabilities.

Running the Latest Versions of modules

Running the latest version of Drupal alone is not enough to secure your site. Modules you install on your Drupal site that contain vulnerabilities will undoubtedly increase your site's attack surface.

Therefore, making sure that your Drupal modules are up-to-date is essential. In doing so, you can make sure your site is covered with the latest security updates by the extension's author.



Drupal (Core) Updates Screen

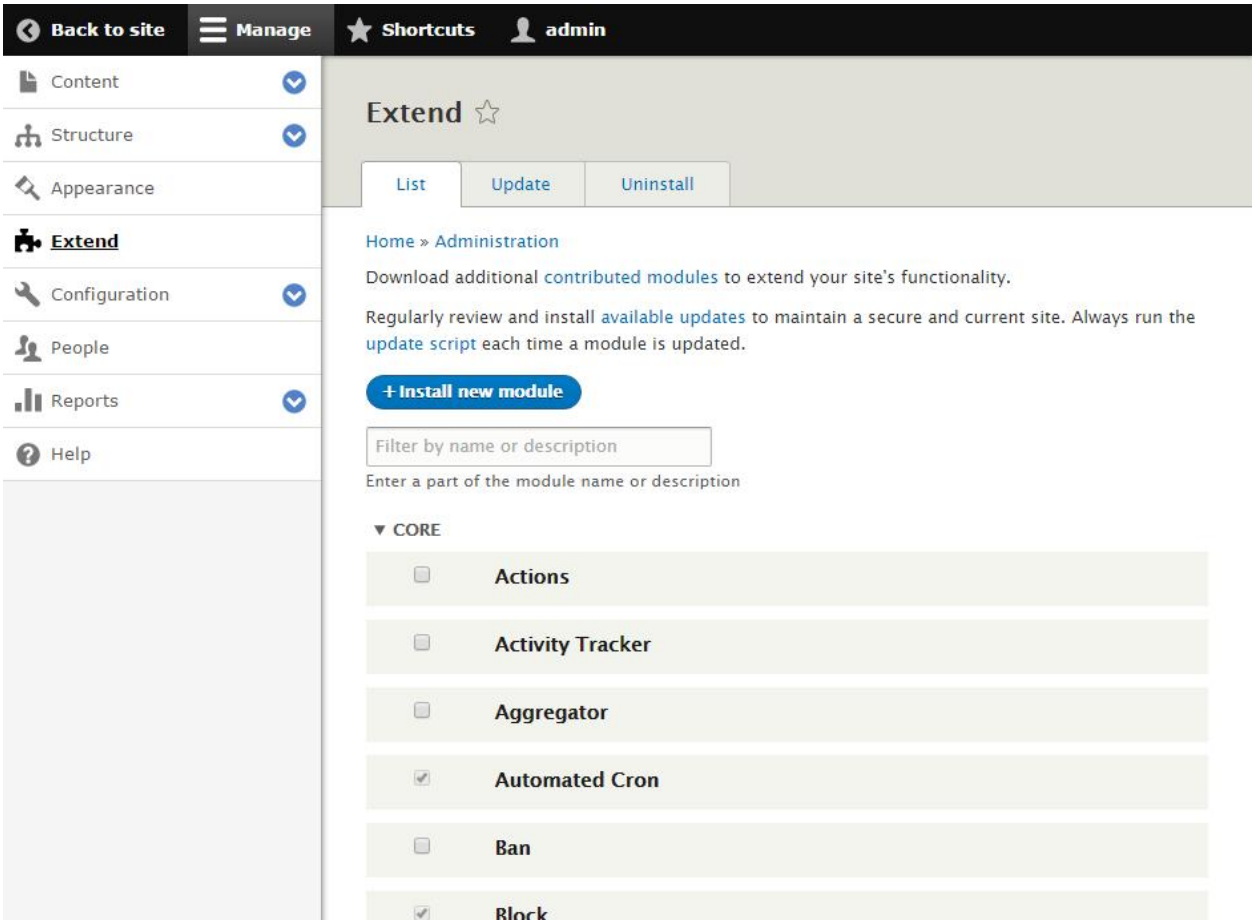
Be Selective When Choosing Modules

Drupal allows you to extend and customize your site with thousands of *modules*. Extending your site's capabilities and customizing it to your requirements is important, however, it should never come at the price of your website's security.

Even if your Drupal installation and modules are all up to date, it does not mean that a site is not vulnerable to attack. Attackers can try to enumerate installed modules to discover what modules you have installed on your Drupal site. By avoiding the installation of unnecessary modules, you would automatically be reducing your site's attack surface.

When choosing modules to install, be selective. Before installing an extension, read about it (ideally read reviews from other users on websites other than the extension developer's site). This prevents you from installing malware or modules that do not fit your purpose.

Check how many downloads the extension has and when it was last updated by its authors. The more downloads and recent updates the extension has, the more likely it is for a vulnerability found, to be fixed quicker.



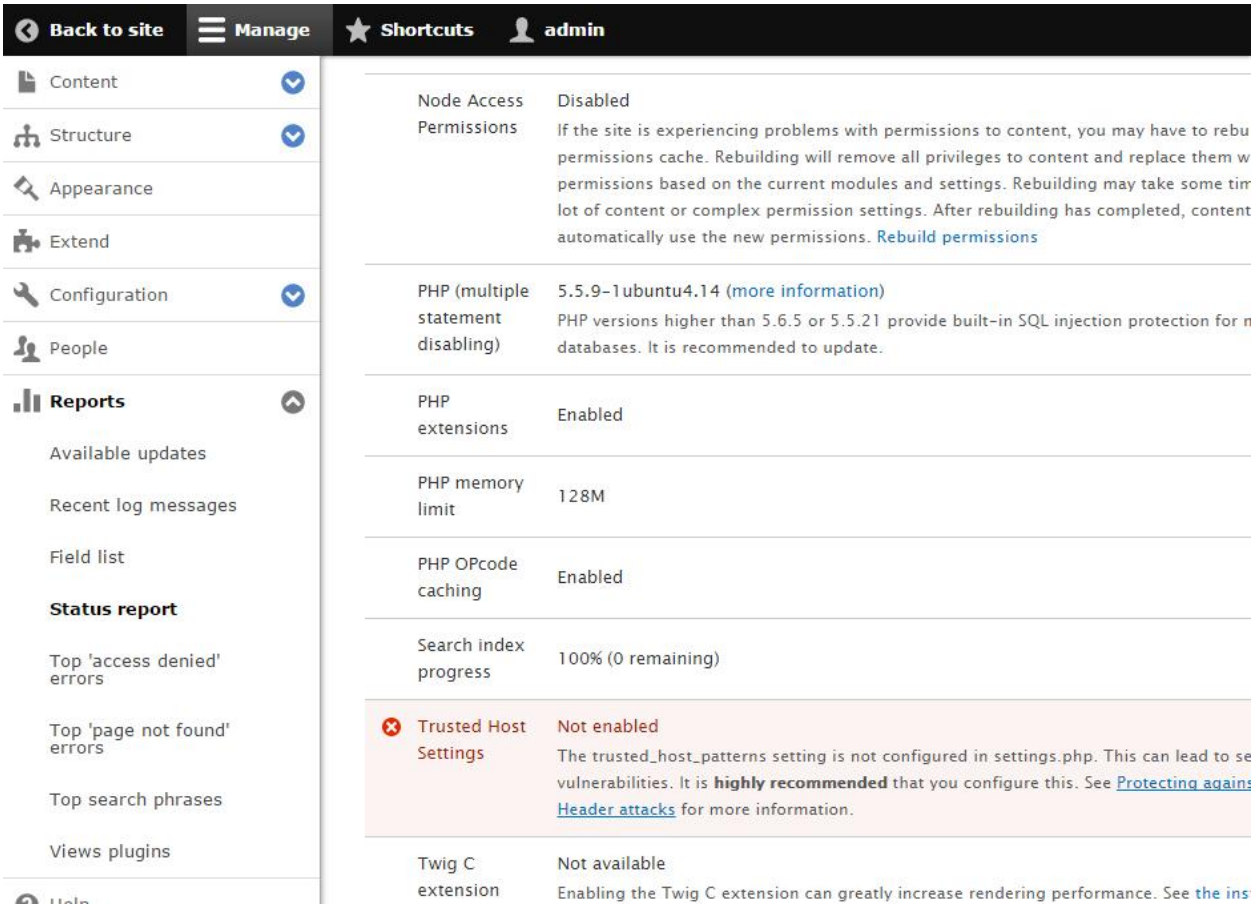
Remove Inactive Users

Keeping inactive users on your Drupal site increases your attack surface. Users, especially Administrators and others who have the ability to modify content, are possibly one of the weakest points of any site because unfortunately, most users tend to choose weak passwords.

If you absolutely need to keep inactive users in your Drupal database, change their role to 'Authenticated user' in order to limit any actions that could be performed.

Take advantage of Drupal's *status report* functionality

A great security feature to take advantage of in Drupal is it's in-built *status report* page. Apart from allowing you to keep tabs on other areas of your Drupal site, the *status report* page, provides you with visibility into some important security controls that you should be placing on your Drupal site — for example, the screenshot below indicates that we need to set-up a list of *Trusted Host Settings* to prevent the possibility of a host header attack from occurring.



Configuring Trusted Host Settings

Drupal has a feature that tries to automatically figure out the base URL of the site. Unless explicitly configured. This can result in a host header attack taking place, specifically because the 'host' HTTP header can be forged by an attacker and therefore cannot be trusted.

Fortunately, Drupal has a built-in method of working around this issue by explicitly defining which hostsnames are to be accepted as valid host headers. This can be achieved by adding the following to your Drupal site's settings.php.

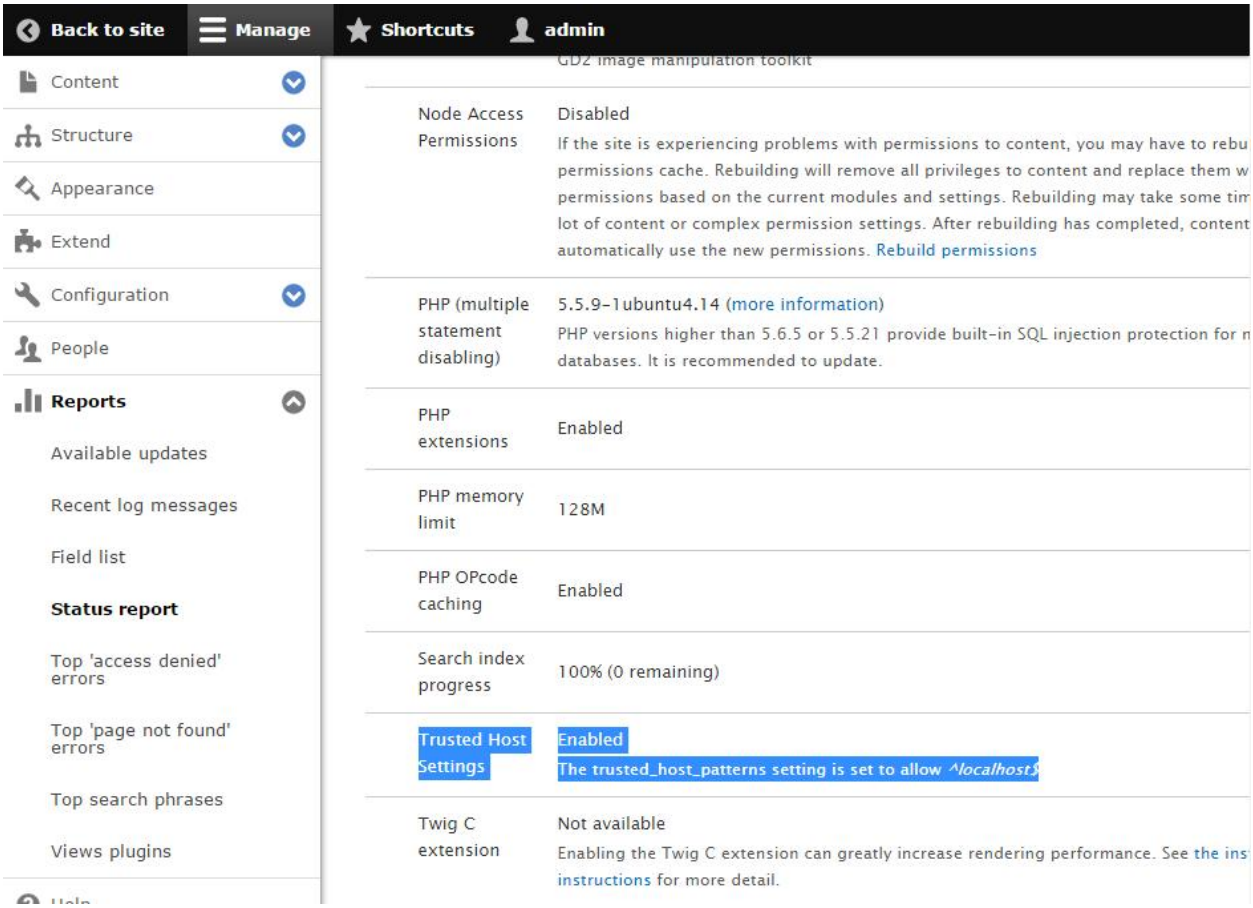
If a site is run off of a single, canonical domain, then you can include the following in sites/default/settings.php to allow the site to only run from *www.example.com*.

```
$settings['trusted_host_patterns'] = array(
  '^www\.example\.com$',
);
```

If you need to run a your site off of multiple domains, and are not redirecting to a singular domain, then you can include the following in settings.php to allow the site to run off of *example.com* and *example.net*, with all subdomains included.

```
$settings['trusted_host_patterns'] = array(
  '^example\.com$',
  '^.+\.example\.com$',
  '^example\.net',
  '^.+\.example\.net',
);
```

If we revisit Drupal's status report, we can see the alert in the previous screenshot resolved.



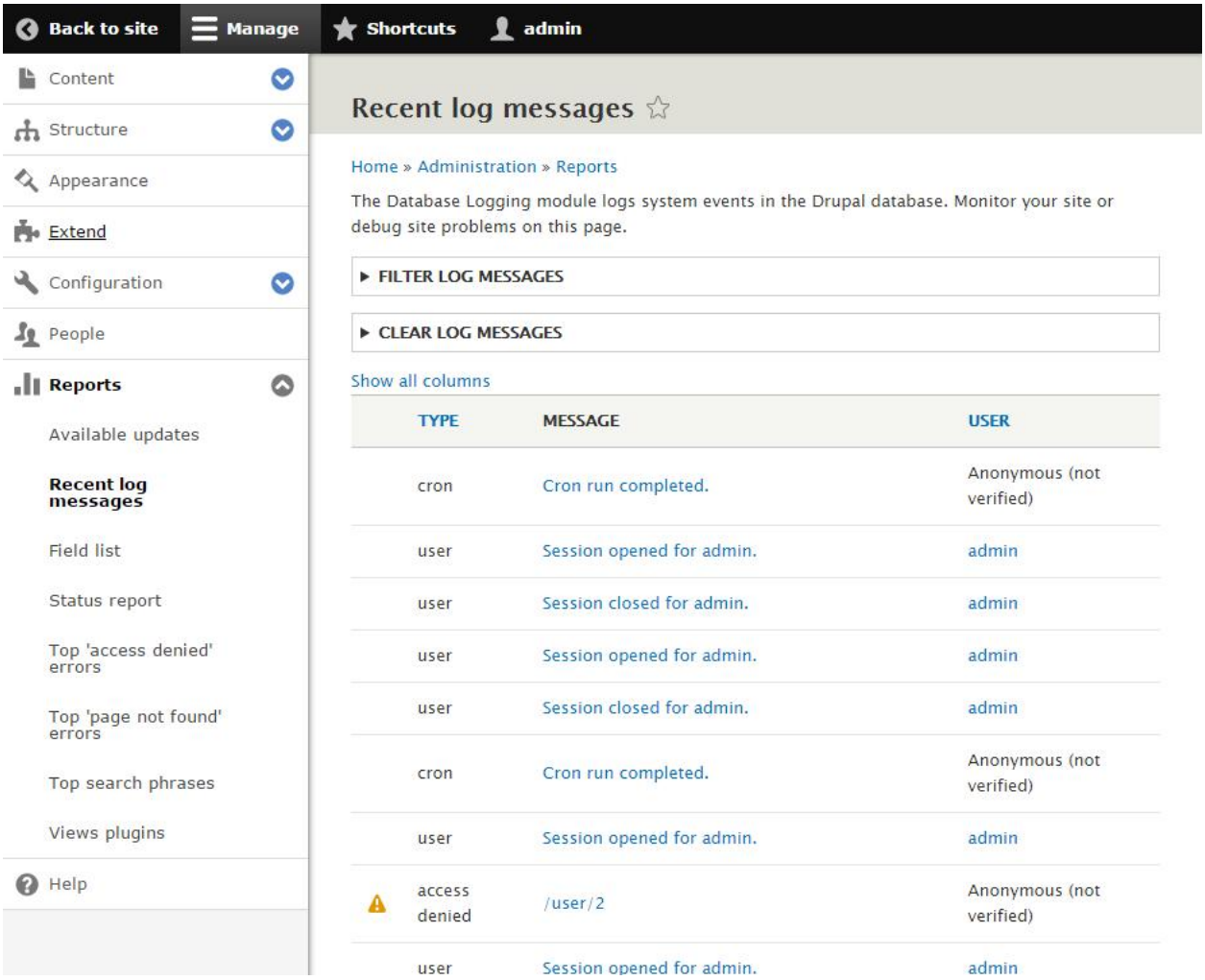
Security Configurations

Heads up - Depending on your webserver's configuration for active modules, the following could break some functionality. It is strongly advised to try out any configuration in a testing/staging environment before changing any configuration on production servers.

Keep an eye on the logs

Drupal has an in-built log viewer (Manage > Reports> Recent log messages) which you should certainly take advantage of. Logging plays a crucial role in understanding when an attack is underway and what has happened after an attack occurred.

By keeping an eye on logs, you can mitigate the the effects of a security breach by paying attention to early warning signs such as failed login attempts.



Enable HTTPS

Strictly speaking, HTTPS is not a protocol in and of itself, but it is rather HTTP encapsulated in TLS/SSL. TLS, or SSL, as it is commonly referred to, provides websites and web applications with encryption of data being transmitted and authentication to verify the identity of a host.

HTTPS is usually synonymous with shopping carts and Internet banking, but in reality, it should be used whenever a user is passing sensitive information to the web server and vice-versa.

Most sites do not necessarily need to serve their entire site over TLS, however, since Drupal does not have an administrator-specific area, it's strongly advised that TLS/SSL is not only implemented, but enforced.

In order to enforce TLS/SSL on your Drupal site in Apache HTTP Server, you will need to add the following configuration in your Drupal site's .htaccess file (this is usually located in your website's root directory).

Note - You must already have TLS/SSL configured and working on the server before your site will work properly with these settings applied.

```
# Force HTTPS across the Drupal site
<IfModule mod_rewrite.c>
  RewriteEngine on
  RewriteCond %{HTTPS} off
  RewriteRule (.*) https://%{SERVER_NAME}$1 [R,L]
</IfModule>
```

About the Author

Ian Muscat – Product Communications Manager at Acunetix

Ian works closely with the Product Team, contributing to research efforts and published material. Ian has previously been part of Acunetix' Technical Support and Quality Assurance Teams, supporting various Fortune 500 companies and government organizations internationally.

He was part of several scoping interactions around the application of web application security tools into the SDLC. Ian is a frequent author on Acunetix' Web Application Security Blog and is particularly interested in the emerging global web application security climate and new web technologies.

@ianmuscat

www.acunetix.com

Network Security in 2016: Let's be Prepared

By Narendran Vaideeswaran, Product Marketing Manager, SolarWinds

There will be an estimated one million cybersecurity job openings in 2016, according to a recent report from Cisco. This is good news for both seasoned IT security experts and up and coming network and security professionals. It also shows that more companies are planning to take network security seriously in 2016. And it's for good reason: according to Kroll's data security statistics, today's average cost of a data breach is $5.9 million.

But this begs the question: What exactly can you do to help ensure your organization's networks, other critical infrastructure and potentially sensitive data stay safe this year and beyond? Here are ten tips and considerations that answer that question, whether you're a seasoned IT security pro or aspiring to become one.

Prepare the security framework

What does your current security framework look like? If you don't have one, start with a comprehensive audit of the available inventory, including your network's user accounts, type of transactions (public/internal), sensitivity of the data being handled, account roles/responsibilities, BYOD policies and change management policies. And remember, IT security is not necessarily achieved by just one person, machine or policy. The management process depends on a multitude of factors ranging from people, processes and data, and only ends with technology—all designed and working together to accomplish the broader goal. Naturally, this framework will be continuously evolving.

Automate threat detection and response

Users, devices and applications generate a large number of network connections, data transactions and application requests. Manually detecting threats in this cacophony is nearly impossible considering how sophisticated hackers and malware have become. Centralizing syslogs and events from network devices, servers, applications, databases and users via a security information and event management (SIEM) software is a must. Such a tool can automate threat detection and provide corrective responses to mitigate risk. It's just one tool that should be a part of your defense-in-depth armory, others include anti-malware, firewalls (including firewall management), intrusion prevention and threat intelligence (more on this to come).

Implement data-driven analysis

It's possible to detect suspicious network activity if you have access to real-time network data showing there's an increase in Web traffic activity on a critical router or firewall, or suspicious

connection requests from an unknown source outside the network. When an attack happens, data-driven analysis will also help with forensics and root-cause analysis to better understand how the attack happened, where it started and if it's spread further onto the network.

Monitor endpoint devices

Suppose you are a payroll processing company, potentially storing confidential client data. A malicious insider at your company could be saving this sensitive data to a USB device and taking it with them, right under your nose. To mitigate his threat, ideally, you should be monitoring all endpoint devices, be it a laptop, USB drive or any other. Back to our example, with proper device monitoring, as soon as the user plugs in the USB device, the device could be ejected/blocked automatically and a corrective action, such as a warning message or account blocking, implemented.

Demonstrate PCI DSS and HIPAA compliances

Payment card and healthcare industries are more prone to data breaches than most others because a single attack has the potential to compromise data from millions of credit cards or patient records. Given the extra sensitive data, it's important to automate and demonstrate compliance with required standards, such as PCI DSS and HIPAA, to avoid regulatory fines or criminal proceedings and protect your servers and databases.

Even if you're not operating in an industry required to meet these or other compliance standards, it's never a bad idea to operate as though you are, leveraging the standards as guidelines for the bare minimum you should be doing (remember, compliance alone does not equal secure).

Identify insider threats

It's entirely possible that the most damaging security compromise may happen from the inside. Dedicated monitoring of network traffic, logs, credentials and which users attempted to access server data should be commonplace. For example, such monitoring could flag an employee attempting to log into a business critical server or core router they have no need accessing.

Beware of ransomware and other social engineering threats

Ransomware is a type of malware gaining steam that locks your files or systems with an encryption that can only be decrypted after paying a ransom. Beware of notorious ransomware families like CryptoWall 3, CryptoLocker and CTB-Locker. It's just one type of threat that often leverages social engineering to trick users into taking actions that ultimately compromise their device(s) and your network.

Educate your users on the ill-effects of instantly opening an email attachment or clicking “OK” to run unknown executables.

Look for file integrity changes

Subtle changes to files, registries and data can be hard to detect, and most zero-day threats use this to their advantage. File integrity monitoring is an important tool to identify stealthy changes to files and registries, and will prevent data loss and business downtime.

Enable threat intelligence

Most common attacks are spread by corrupt hosts on the Internet. Collective intelligence on these bad actors can be utilized to proactively pinpoint security concerns like potential phishing attempts and infections. By closely monitoring suspicious traffic going to *known* command and control servers, there’s a greater chance you’ll be able to catch a threat before it infiltrates critical infrastructure.

Practice knowledge sharing

Knowledge sharing among your peers and educating users on common attack types, phishing sites and malware infections can fortify your security framework to a much greater extent than you might think. The threat landscape is constantly evolving, and collective knowledge helps in proactively avoiding common threats.

In short, 2016, with an ever increasing number of users, data and network connections, is going to be more challenging than ever from a cybersecurity perspective. However, with the right security strategy and tools, you can rest easier knowing you’ve taken the proper steps toward being better prepared to combat threats.

About the Author

Narendran Vaideeswaran, Product Marketing Manager, SolarWinds

Naren Vaideeswaran is a product marketing manager at SolarWinds for the company’s security portfolio. A technology enthusiast, he has worked in the IT and security industries for over a decade in both technical and marketing roles.

Preventing DNS-Based Data Exfiltration

By Cherif Sleiman, General Manager, Middle East at Infoblox

Summary: Theft of sensitive or regulated data and intellectual property is one of the most serious risks to an enterprise. DNS is frequently used as a pathway for data exfiltration, because it is not inspected by common security products such as firewalls, intrusion detection systems (IDSs), and proxies.

Several high-profile data breaches have been in the news recently. We read that millions of customer records are stolen, emails hacked, and sensitive information leaked. Most enterprises have multiple defense mechanisms and security technologies in place, such as next-generation firewalls, intrusion detection systems (IDSs), and intrusion-prevention systems (IPSs). Yet somehow malicious actors find a way to appropriate data. So what types of data are being stolen? They vary and may include:

- Personally identifiable information (PII) such as Emirates ID numbers in UAE for example
- Regulated data related to Payment Card Industry Data Security Standard (PCI DDS)
- Intellectual property that gives an organization a competitive advantage
- Other sensitive information such as credit card numbers, company financials, payroll information, and emails

Motivations vary from hacktivism and espionage to financial wrongdoing, where the data can be easily sold for a neat profit in the underground market. When sensitive information is stolen, it causes financial and legal woes, not to mention the huge negative impact to brand. According to a Ponemon Institute study in 2015, the average consolidated cost of a data breach is US$3.8 million, which includes investigative and forensic efforts and resolution and consequences of customer defection. This is an average—recent breaches have cost victims a lot more.

Hackers can use multiple pathways to steal data, but the one that is often unknowingly left open is DNS, or the Domain Name System. DNS is increasingly being used for data exfiltration, either by malware-infected devices or by rogue employees. The nature of the DNS protocol, which was invented more than 30 years ago, is such that it is trusted, yet vulnerable to hackers and malicious insiders. According to Dan Kaminsky, the a well-known DNS security researcher, DNS can be thought of as a globally deployed routing and caching overlay network that connects both the public and private Internet, which raises serious questions: Is it sufficiently secure? Is it vulnerable to data breaches?

The answer is that DNS can be abused in all sorts of unconventional ways that make it the perfect back door for hackers seeking to steal sensitive data. According to a recent DNS security survey of businesses based in North America and Europe, 46 percent of respondents experienced DNS exfiltration and 45 percent experienced DNS tunneling. You can safely assume that the Middle East will be no different.

DNS tunneling is the tunneling of IP protocol traffic through Port 53—which is often not even inspected by firewalls, even next-generation firewalls—most likely for purposes of data exfiltration. Malicious insiders either establish a DNS tunnel from within the network, then encrypt and embed chunks of data in DNS queries. Data is decrypted at the other end and put back together to get the valuable information.

All sorts of things can be tunneled (SSH or HTTP) over DNS, encrypted, and compressed—much to the dismay of network administrators and security staff. DNS tunneling has been around for a long time. There are several popular tunneling toolkits such as Iodine, which is often considered the gold standard; OzymanDNS; SplitBrain; DNS2TCP; TCP-over-DNS; and others.

There are also newer contenders that allow for tunneling at a much faster pace and offer lots of features. Even some commercial services have popped up offering VPN service over DNS, thus allowing you to bypass many Wi-Fi security controls. Most of these tools have specific signatures that can be used for detection and mitigation.

DNS is not only used for data leakage, but also to move malicious code into a network. This infiltration is easier than you think. Hackers can prepare a binary, encode it, and transport it past firewalls and content filters via DNS into an organization's network. Hackers send and receive data via DNS—effectively converting it into a covert transport protocol.

Don't Become the Next Data Breach Victim

DNS is the perfect enforcement point to improve your organization's security posture. It is close to endpoints, ubiquitous, and in the path of DNS-based exfiltration. While DLP technology solutions protect against data leakage via email, web, FTP, and other vectors, most don't have visibility into DNS-based exfiltration. To maximize your chances of fighting back against these data theft attempts, complement traditional data loss prevention protection with a DNS- based solution.

About the Author

Mr. Sleiman has more than 20 years of sales, technical and business experience with some of the world's leading networking and telecommunications technology companies. He has held key executive roles, including chief operating officer and chief technology officer at Core Communications, a software and IT services company focused on cloud-based business services and web and mobile apps. He spent more than six years at Cisco in various leadership positions, the last being senior director, leading the enterprise business for Middle East and Africa. He also developed the strategic vision and technology roadmap, and managed all aspects of research and development, for Nortel Networks in his role as CTO, Enterprise Business Unit.

Be aware or you may become a victim of Ransomware

By Prerna Lal, Faculty, International Management Institute, New Delhi, India

Recent news regarding WordPress sites being hacked to deliver crypto ransomware to unwitting end users, Oxford school computers being hacked with ransomware, and Hollywood Presbyterian Medical Center getting hit with ransomware are alarming as these incidents are increasing with unprecedented numbers.

Ransomware is a type of malware that often infiltrate systems and prevent or limits users from accessing their system or may even encrypt victim's files. Attackers then force victims to pay ransom to get access to the system or decrypt data files. The ransom is often paid in form of electronic currency, such as bitcoin, which is very difficult to track.

How ransomware works?

Ransomware gets gain access to into the victim's computer in a number of ways; it can get downloaded unknowingly by visiting a malicious or compromised website, or by clicking on an infected popup advertisement, or downloading an effected attachment, or by getting tricked into purchasing a fake antivirus software. Once it is downloaded, it takes the victim's computer hostage. Subsequently, it may either lock the victim's computer or encrypt various types of files (e.g., doc, jpg, etc.). Finally, attackers put pressure on the victim to pay as demanded within a specified time failing in which their data will be destroyed or posted on the Web.

How serious the threat is?

Past few years have witnessed the tragic suicide by UK teen after receiving a bogus "police" email which claimed he had been browsing illegal websites and had to pay ransom £100 or face being prosecuted. In another incident, Romanian ransomware victim committed suicide with his 4-year-old son after receiving similar email which deceptively informed him he needed to pay a fine for downloading porn or risk going to jail.

Other than individuals, organizations are also becoming a target of ransomware. Criminals are finding it more lucrative as they demand millions of dollars to unlock or de-crypt the organizational data. For organizations, data is critical be it hospital, bank, or school, and moreover, if systems are down for even few hours, it may harm their business as well as reputation. Criminals take advantage of this by attacking organizations and demand a large sum of money.

Recent advancements such as introduction of the Internet of Things (IOT) are more vulnerable to ransomware attacks resulting in hacking and ceasing our day to day operations. On one hand, IOT helps individuals as well as organizations in managing their security, lights, machines or appliances through a system or even a mobile device. While, on the other hand, if cyber criminals get hold of these systems and are able to lock them, then it may lead to a very grave

situation where in the victim will be forced to pay ransom even to get out of/ in the office/ house or use machines.

What can we do to ensure protection from ransomware?

It is always better to take precautions and protect systems than becoming a victim in the first place. Here are few suggestions:

- The first and foremost step is to ensure installation of an authenticated anti-virus software.
- Ensure regular backup of system data.
- Check twice before downloading an attachment as it may carry ransomware.
- Enable popup blocker to avoid accidently clicking on infected popup advertisement.
- Ensure that you are accessing trusted websites.

In case someone is affected by ransomware the first thing to do is to disconnect the internet as soon as possible to avoid transaction of your system data to the criminals. By doing this one can always use backup data for resorting the system.

In a study conducted by security solutions provider Bitdefender it was discovered that 4 in 10 ransomware victims pay ransom to recover data. This is not considered a good decision by experts as they suggest that informing authorities about the attack is always better option than paying ransom. Paying ransom may encourage criminals which may lead to victims being subjected to similar attack for extorting large amount next time.

Stay vigilant

According to a report from Intel Corp.'s McAfee Labs, with the upcoming new cloud-based variants of ransomware i.e. "ransomware-as-a-service", ransomware will remain a major and rapidly growing threat in 2016. Individuals as well as organizations should be ready for dealing with such attacks with proper security implementations. Further they should also educate and update themselves regarding latest cybercrimes and stay vigilant and don't let hackers win and control their lives.

About the Author

Prerna Lal is a Lecturer in Information Management at International Management Institute, New Delhi and a published writer in journals and publications, both Indian and international. She is an engineer with an MBA degree (IIT-Roorkee). She is a SAP-certified consultant (HCM) and has ITIL® V3 Foundation-level certificate in IT Service Management as well as Diploma in Cyber Law. She has 14 years of experience in academics and research with areas of interest being Data Warehousing and Data Mining, Business Analytics, Cyber Law, Management Information System, Software Project Management, IT Service Management, and Cloud Computing. She can be contact at prernalal@yahoo.com.

Visualize the Cyber Arms Race. What Does a Hack Attack Really Look Like?

By, Todd Helfrich, Director of Federal, ThreatStream

When you hear the phrase “cyber warfare,” do you envision a lone figure hunched over a flickering monitor in a dark corner? Or perhaps a sleek control room staffed by nefarious characters, executing orders issued by a despotic computer genius?

Now, using ThreatStream Lab’s Modern Honey Network (MHN), cyber investigators can watch actual cyber-attacks as they happen. Not the criminals behind the keystrokes, but the real-time cyber events that happen inside and outside of a system when it is being assaulted.

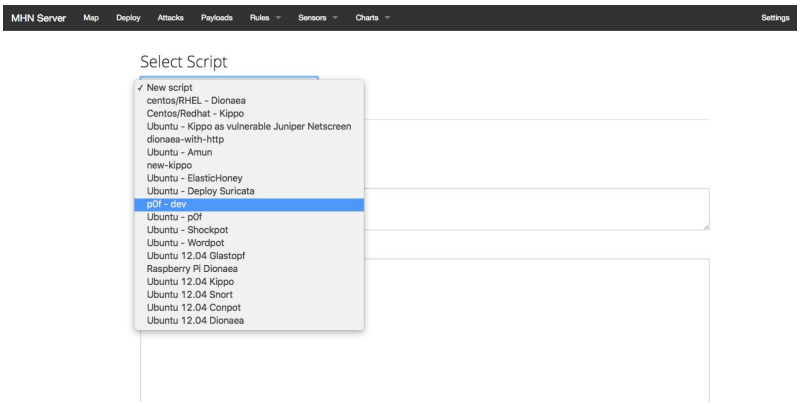
ThreatStream’s honeypots are disguised as vulnerable servers, laptops or networks. The devices act as lures to attract attacks, so cybersecurity experts can study the techniques hackers use to breach cyber information systems.

Honeypots are not a new weapon in the cyber arms race. But MHN makes it easier than ever to deploy and maintain decoys, and it automates the incorporation of collected threat intelligence into cybersecurity tools. Installation and management of honeypots is streamlined. Setting up data flows, analyzing collected data and making it actionable is simplified.

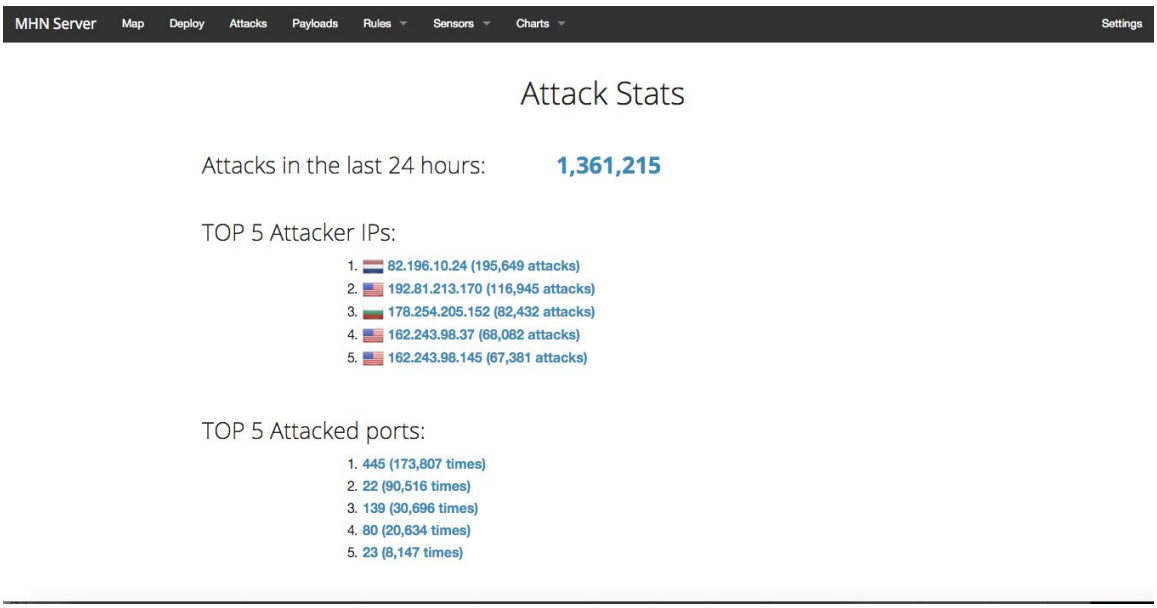
Just as hackers learn from defensive measures, revealing how the bad guys operate enhances cybersecurity protections. Let’s take a trip to the dark side, and see a honeypot in action.

Like Bees to Honey, the Buzz Is Almost Instant

Using MHN is no different from the interfaces IT consumers have come to expect from cloud-based applications. Once inside, a cyber assault is just a few mouse clicks and a screen refresh away.

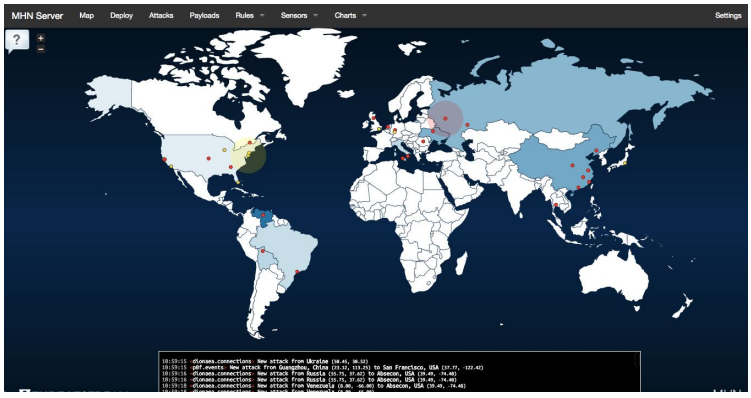


Implementation can be as simple as choosing a preprogrammed, bare-bones honeypot from a dropdown menu. Or, custom lures can be designed and deployed based upon the type of information to be collected.

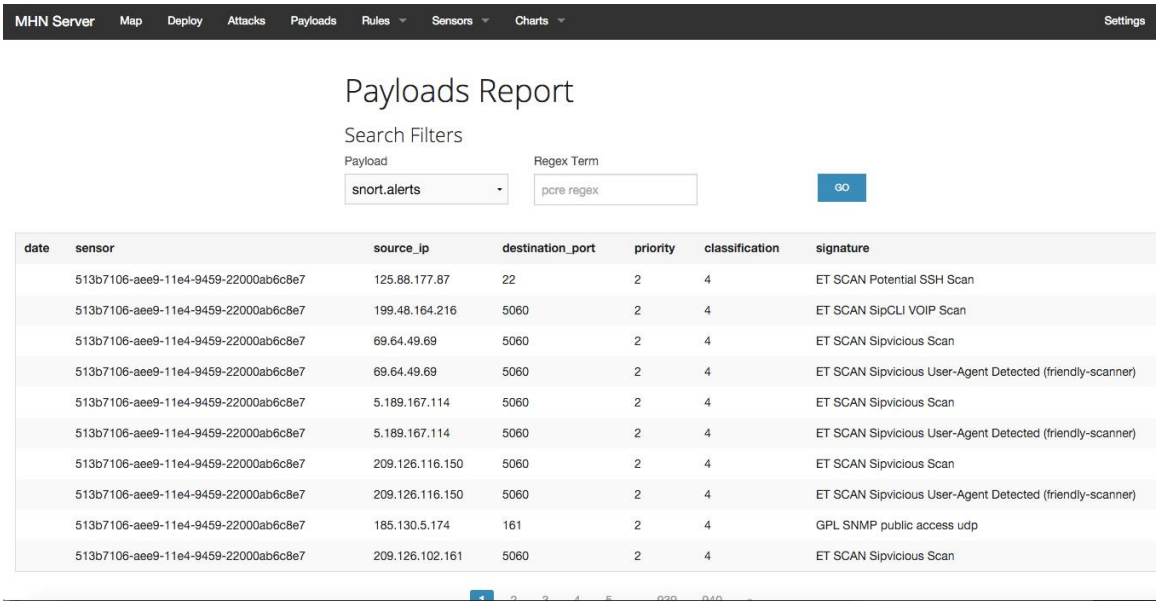


What types of phishing scams are hot right now, or what are the most active and dangerous sites? Which ports are popular? Honeypots have different characteristics that lure and capture specific types of traffic, and therefore, intelligence.

MHN is an open source project; users are encouraged to feed it events while becoming a part of a larger sensor grid. MHN low-interaction honeypots can be placed on the perimeter of a network—to see who's trying to break in—or deep into protected spaces. Deployed inside of a network, honeypots can catch compromised hosts that are internally scanning your network or detect a malicious insider doing something they should not be doing. A honeypot acts as early warning system.



Once launched, a honeypot can attract attention in mere seconds. Blinking red dots, correlated with IP geography, are scattered across the MHN global map. It visualizes the bad bees buzzing around the new, exposed hive, the yellow beacon. All the while, those bees are revealing source IP, destination ports, signatures, protocols and more, in a detailed, scrolling log at the bottom of the map.



MHN examines HPfeeds flowing from the sensors, extracts information about the attacker, and collects metadata about the type of honeypot that was attacked.

The collective brain power of open source tools including nmemosyne, honeymap, Mongo DB, Dionaea, Conport, Snort, Suricata, Kippo, among others, are used to gather, organize, analyze and store threat intelligence.

When users designate sharing, that information is funneled to the MHN community hub. MHN provides full REST API out of the box.

CEF and STIX support are available for direct SIEM integration through ThreatStream's commercial platform, Optic™. MHN also generates user-friendly reports that support attack trend analysis. (The crowd-favorite report tends to be the list of most easily compromised passwords.)

You are creating—and watching—cyber vapor, the trail of evidence left behind by the adversary. This is a hack attack in action.

Share the Honey But Don't Get Stung

Sleuthing can be dangerous work. The key to a successful honeypot is that hackers never realize they've encountered a honeypot.

While MHN is a community-based project, it employs a strict management hierarchy that evaluates code, contributions, sensors and trust relationships, to protect the reliability of MHN data.

And remember, the intelligence gathered through MHN is only as good as far as it is disseminated. Users are not required to share the data they collect; many honeypots are deployed in sensitive environments.

But the platform enables users to manage and share threat indicators, with the goal of crowdsourcing data to increase cybersecurity protections. As one user finds information relevant to their vertical, they can push it into the platform and share it with a larger community.

Honeypots have not received wide adoption as an enterprise defense largely because the deployment and management has been a complicated process reserved for security companies and security researchers.

Now with MHN, cybersecurity professionals have access to an enterprise-ready honeypot management system, which enables organizations to create a fully functional, active-defense network in minutes. It's pretty sweet.

NOTE: To learn more about The Modern Honey Network, visit ThreatStream's website. ThreatStream's honeypot software is open source and is available for free to cybersecurity specialists.

THE COMMERCIAL UAV SHOW ASIA 2016

1 – 2 September 2016,
Suntec Convention Centre,
Singapore

DEMONSTRATING REAL WORLD APPLICATIONS OF UAV'S

Join over 1,000 industry leaders and regulators from across Asia as they share valuable case studies on their experiences and success in applying unmanned technologies. Learn from the likes of BP, SCION, University of Adelaide and many more as they discuss how UAV's help them save money, time and lives.

This 2nd annual event is a must attend for anyone looking to make the right connections in Asia's unmanned systems market.

FEATURED SPEAKERS

Claus Nehmzow,
Digital Innovation Organization,
BP, Singapore

LianPin Koh,
Associate Professor, Chair of Applied Ecology and Conservation,
University of Adelaide, Australia

Bryan Graham,
Science Leader, Forestry Industry Informatics,
SCION, New Zealand

TOP SPONSORS & EXHIBITORS

SPONSORS:

AltaDevices · delair-tech · senseFly a Parrot company · YUNEEC AVIATION TECHNOLOGY

EXHIBITORS:

INFINIUM ROBOTICS · Keii 科易光电 · - when it has to be right · Leica Geosystems · ALT · Silvertone · UNIFLY

QUOTE CYDEF and get 10% off the final price
Book now at **www.terrapinn.com/uavasia**

The ESIS Encryption Law

Abstract: *In this article, I introduce a completely new system of multi-level encryption which can provide a unique solution for the given set of input information. This new method is defined using a set of the rules which are governed by the ESIS Encryption Law. In this case, an ESIS means External-Symmetric Internal-Single. In other words, this corresponds to external bits of encrypted information which are the results of symmetric function applications and internal bits which stay single or in affirmation or in negation. Symmetric functions which are applied in this law are XOR and XNOR functions. A detailed analysis and examples of the ESIS Encryption Law are presented in this paper.*

Introduction

It is considered that Claude E. Shannon is the father of mathematical cryptography. He was working for several years at Bell Labs, and during that he produced an article called *"A mathematical theory of cryptography"* which was published in the Bell System Technical Journal in 1949. Shannon continued his work by writing another article named *"A mathematical theory of communication"*. It is published in 1949 and it considered being the starting point for development of modern cryptography. Shannon obtained the two main goals of cryptography: *secrecy* and *authenticity*. Later, G. J. Simmons addressed the issue of *authenticity*. Shannon's paper *"A mathematical theory of communication"* brought cryptography's transition from art to science.

A secrecy system can be formulated as a set of transformations of one space which addresses to the set of possible messages into another space which addresses to the set of possible cryptograms. Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are reversible. That means the unique deciphering is possible when the key is known. Each key and transformation is assumed to have the probability of choosing that key. Similarly, each possible message is supposed to have a probability which is determined by the underlying stochastic process. These probabilities are actually the cryptanalyst's probabilities for the choices in question and represent the knowledge of the situation.

The ESIS Encryption Law

Since the beginning of my research until the moment of formulating this rule, the way I had to pass was pretty winding. I started my research by examining logic functions and very soon I have noticed that symmetric functions such as XOR and XNOR give a set of symmetric solutions. On the other hand, basic functions such as AND, OR and NOT or combined functions like NAND and NOR provide the set of solutions which is usually repeated. The question which I was asking myself was – "Is there any algorithm which will give a unique set of encrypted information for the certain set of input information?". After some time, I have noticed that external bits of encrypted information must be the result of symmetric function application, otherwise the encrypted information will get deformed. But, the new question was – "Which

function should be applied in order to get a unique set of encrypted information?". I have continued testing the opportunities and very soon the answer to that question appeared. Internal bits should be the result of affirmation or negation or, in other words, they correspond to a single-bit function. Consequently, I have realized that findings can be used for multi-level encryption of digital information.

The fundamental principles of this law are presented as follows. The entire law can be broken down into three cases – two general and one that is the combination of the previous two.

Case 1: ***External XORed, Internal inverted***

In this case, all external bits of the information which is the part of a set of encrypted information are XORed, while all internal bits of the encrypted information are inverted. This is described using a Theorem 1.

Theorem 1

Let assume that we observe a set of *m*-bit binary information, where $m \geq 3$. The set of information contains 2^m different combinations of 0s and 1s. In that case, the source message can be represented using the weight coefficients. This is given in Equation (1).

$$Message = f_n f_{n-1} f_{n-2} \cdots f_2 f_1 f_0 \tag{1}$$

Where:

n - the highest value of the weight coefficient for the message; $n \geq 2$,

f - the weight coefficient for the message.

Let also assume that an encrypted message or a cipher can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (2).

$$Cipher\left(Message\right) = g_n g_{n-1} g_{n-2} \cdots g_2 g_1 g_0 \tag{2}$$

Where:

n - the highest value of the weight coefficient for the encrypted information $n \geq 2$,

g - the weight coefficient for the encrypted information.

If the following algorithm is applied, the result will be a unique set of encrypted information that can be encrypted in more levels.

The 1st Level of Encryption:

Let again assume that an encrypted message in the first level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (3).

$$Cipher1\left(Message\right) = g_n g_{n-1} g_{n-2} \ldots g_2 g_1 g_0 \tag{3}$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

g - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$\begin{aligned} g_0 &= f_0 \oplus f_1 \\ g_1 &= \overline{f_1} \\ &\ldots \\ g_{n-1} &= \overline{f_{n-1}} \\ g_n &= f_n \oplus f_0 \end{aligned} \tag{4}$$

The 2nd Level of Encryption

Let again assume that an encrypted message in the second level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (5).

$$Cipher2\left(Message\right) = h_n h_{n-1} h_{n-2} \ldots h_2 h_1 h_0 \tag{5}$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

h - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$\begin{aligned} h_0 &= \left(g_0 \oplus g_1\right) \oplus g_2 \\ h_1 &= \overline{g_1} \\ &\ldots \\ h_{n-1} &= \overline{g_{n-1}} \\ h_n &= \left(g_n \oplus g_0\right) \oplus g_1 \end{aligned} \tag{6}$$

…..

The (m - 2) Level of Encryption

Let again assume that an encrypted message in the second level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (7).

$$Cipher_{m-2}\left(Message\right) = j_n j_{n-1} j_{n-2} \ldots j_2 j_1 j_0 \tag{7}$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

j - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$\begin{aligned} j_0 &= \left(i_0 \oplus i_1\right) \oplus \ldots \oplus i_{n-1} \\ j_1 &= \overline{i_1} \\ &\ldots \\ j_{n-1} &= \overline{i_{n-1}} \\ j_n &= \left(i_n \oplus i_0\right) \oplus \ldots \oplus i_{n-2} \end{aligned} \tag{8}$$

Case 2: ***External XNORed, Internal in Affirmation***

In this case, all external bits of the information which is the part of a set of encrypted information are XNORed, while all internal bits of the encrypted information are in affirmation. This is described using a Theorem 2.

Theorem 2

Let assume that we observe a set of *m*-bit binary information, where $m \geq 3$. The set of information contains 2^m different combinations of 0s and 1s. In that case, the source message can be represented using the weight coefficients. This is given in Equation (9).

$$Message = f_n f_{n-1} f_{n-2} \ldots f_2 f_1 f_0 \tag{9}$$

Where:

n - the highest value of the weight coefficient for the message; $n \geq 2$,

f - the weight coefficient for the message.

Let also assume that an encrypted message or a cipher can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (10).

$$Cipher\left(Message\right) = g_n g_{n-1} g_{n-2} \ldots g_2 g_1 g_0 \tag{10}$$

Where:

n - the highest value of the weight coefficient for the encrypted information $n \geq 2$,

g - the weight coefficient for the encrypted information.

If the following algorithm is applied, the result will be a unique set of encrypted information that can be encrypted in more levels.

The 1st Level of Encryption:

Let again assume that an encrypted message in the first level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (11).

$$Cipher1\left(Message\right) = g_n g_{n-1} g_{n-2} \ldots g_2 g_1 g_0 \tag{11}$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

g - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$\begin{aligned} g_0 &= \overline{f_0 \oplus f_1} \\ g_1 &= f_1 \\ &\ldots \\ g_{n-1} &= f_{n-1} \\ g_n &= \overline{f_n \oplus f_0} \end{aligned} \tag{12}$$

The 2nd Level of Encryption

Let again assume that an encrypted message in the second level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (13).

$$Cipher2\left(Message\right) = h_n h_{n-1} h_{n-2} \ldots h_2 h_1 h_0 \tag{13}$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

h - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$
\begin{aligned}
h_0 &= \overline{\overline{(g_0 \oplus g_1)} \oplus g_2} \\
h_1 &= g_1 \\
&\ldots \\
h_{n-1} &= g_{n-1} \\
h_n &= \overline{\overline{(g_n \oplus g_0)} \oplus g_1}
\end{aligned}
\tag{14}
$$

…..

The (m - 2) Level of Encryption

Let again assume that an encrypted message in the second level of encryption can be presented as array of the weight coefficients, where number of digits for the message and number of digits for the cipher are the same. This is shown in Equation (15).

$$
Cipher_{m-2}\left(Message\right) = j_n j_{n-1} j_{n-2} \ldots j_2 j_1 j_0 \tag{15}
$$

Where:

n - the highest value of the weight coefficient for the encrypted information; $n \geq 2$,

j - the weight coefficient for the encrypted information.

The algorithm is as follows:

$$
\begin{aligned}
j_0 &= \overline{\overline{(i_0 \oplus i_1)} \oplus \ldots \oplus i_{n-1}} \\
j_1 &= i_1 \\
&\ldots \\
j_{n-1} &= i_{n-1} \\
j_n &= \overline{\overline{(i_n \oplus i_0)} \oplus \ldots \oplus i_{n-2}}
\end{aligned}
\tag{16}
$$

Case 3: ***A Combination of the Previous Two Cases***

In this case, the set of encrypted information is the result of the combination of the previous two theorems.

Further, I encourage all the curious researchers and engineers to try to prove this law using, for instance, a set of 4-bit binary information. As it can be shown, solutions of such a multi-level

encryption are unique. At this stage the ESIS Encryption Law has been formulated completely which no doubly opens limitless possibilities in this field of mathematics and binary logics.

Discussions

All the findings and results provided in this article could be used for the real cryptographic purposes. For instance, using proposed algorithms or the knowledge about this law, it would be possible to design hardware for encryption or even develop software for that purposes. This could be the beginning of the big project which would be governed by results provided into this study. In the future, maybe this idea could be used for development of some communication protocol which would be cryptographically protected using such or similar algorithms and rules. In other words, all the results given here have a strong practical meaning and could be used for technical, engineering and programming purposes.

Conclusion

In conclusion, the field of discrete mathematics is the exciting one. There are a lot of information and knowledge waiting for us to discover them. I strongly encourage all the future researchers and scientists to spend some time examining and testing logical functions, because their results could find great applications in cryptography, digital systems or even computer science.

References:

[1] Hai Cheng, Qun Ding, 2012, *Overview of the Block Cipher*, IEEE Proceedings
[2] Jim Geler, 2010, *Designing and Developing 802.11n Wireless Networks*, Cisco Systems Inc.
[3] Raphael C.-W. Phan, 2006, *A Framework for Describing Block Cipher Cryptanalysis*, IEEE Transactions on Computers
[4] William Stallings, 1999, *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, Inc., New Jersey
[5] Ronald J. Tocci & Neal S. Widmer, 1998, *Digital Systems – Principles and Applications*, Prentice-Hall International, Inc.
[6] Yan Zhang, Jijun Luo, Honglin Hu, 2007, *Wireless Mesh Networking: Architectures, Protocols and Standards*, Taylor & Francis Group, New York

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia.

She also serves as a Reviewer at the Journal of Computer Sciences and Applications and. She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Security & Counter Terror Expo 2016: An international platform for global security

Leading event returns to London in April with a programme created to help those tasked with keeping nations, assets and businesses safe

Over recent years the threat of terrorism has increased exponentially and today terrorist activity is undertaken on an almost a daily basis. In 2015 alone, there were more than 380 recorded terrorist attacks by violent non-state actors for political or unknown motives.

These attacks are now wide reaching and intercontinental. The Nigerian government is just one example, it has been combating the ever increasing Boko Haram insurgency for over a decade, while elsewhere the undercurrent of political instability in the Middle East continues to be a breeding ground for both Al-Qaeda and the so-called Islamic State.

Yet the advent of global terrorism has not been exclusive to war-torn and typically unstable nations. Over the past 12 months, Europe has played host to some of the deadliest attacks in its history. Paris has been the epicentre of terror activity with Islamic extremists carrying out a series of co-ordinated attacks at six locations, including the Stade de France stadium and the Bataclan Theatre in central Paris.

The threat is constantly evolving and is currently at a significantly high level worldwide. Following recent events in Europe, the issue of national security and counter terrorism is now firmly at the top of government agendas.

Returning to Olympia, London from 19 – 20 April 2016, Security & Counter Terror Expo, will help nations improve border control, critical national infrastructure protection, cyber security, major events, offender management, policing and counter terrorism, and the emergency services. It will showcase the latest cutting-edge technology and provide those tasked with protecting nations and assets with valuable knowledge through a series of conference sessions.

David Thompson, Event Director, said: “The recent global events have reminded us that the security can’t be taken for granted. Targets are becoming more diverse, as are the methods employed by those that seek to do us harm.

“With the safety of millions of people on their minds, security professionals have an increasingly important role to play as the threat evolves. Security & Counter Terror Expo 2016 is aligned with the Home Office’s seven security capabilities and will offer industry experts the perfect platform to source the latest technology, discuss important issues with likeminded peers and hear from the leading voices in security and counter terror policy.”

Innovation at Security & Counter Terror Expo

The exhibition has established itself as an international hub where the industry elite come together to identify the security sector’s most significant innovations and new product launches.

Security & Counter Terror Expo 2016 will showcase a wide range of product innovations from more than 240 exhibitors, including those supplying the latest in high security fencing, cybersecurity modelling, simulation and training platforms, surveillance control systems and drone technology. Geoquip, CLD Fencing, NEC, Aselsan and Jacksons Fencing are among the major multinational companies to already confirm their presence at 2016 show and will join more than 50 new exhibitors offering cutting edge services and security solutions to the industry.

This year visitors will find a number of exciting product launches. Having recently successfully completed 8.5km of security fencing and associated gates at the Eurotunnel Terminal, Coquelles, France, Jacksons Fencing will launch its full range of LPS 1175 SR1 - SR5 security rated fencing systems on stand K40.

Peter Jackson, CEO of Jacksons Fencing, commented: “Security & Counter Terror Expo acts as a broad and direct communication channel to one of our key markets, allowing us to engage with prospects, as well as existing clients. It is a great platform for us to showcase our latest innovations and provides us with a great insight into what’s happening in the security sector – all under one roof.”

Lincoln Security will be launching its latest range of locks, eLOQ, on stand C82. The devices are electronic and contain no wiring or batteries allowing them to be deployed anywhere, instantly. The solution also features unique electronic keys that can be programmed to open locks based on time and date restrictions, while also providing a full audit report of who has unlocked the eLOQ.

Also confirmed, HGH Systèmes Infrarouges will showcase its wide area surveillance systems, for critical infrastructure protection, based on its award-winning 360-degree thermal camera, the SPYNEL, and its automatic intrusion detection and tracking software, CYCLOPE. Speaking about the decision to return to Security & Counter Terror Expo 2016, Gildas Chauvel, Marketing Manager, said: ‘We are able to meet high level, influential security professionals who specialise in protecting critical national infrastructure and homeland security and the show affords us the opportunity to discuss our solutions with potential new customers.”

Discussing new strategies to tackle terrorism

With counter terrorism firmly in the spotlight, more than 400 security professionals from across the globe will attend the high-level paid-for World Counter Terror Congress, from 19 – 20 April 2016. Reflecting the international nature of the exhibition, the Congress will feature speakers from national, international and supranational institutions.

The World Counter Terror Congress will feature six sessions, covering policy and strategy responses to the changing terror threat; radicalisation, de-radicalisation and preventing radicalisation; geopolitical security briefings; encryption, communications and security; security for critical national infrastructure; and emerging terror networks and tactics.

Focusing on the four key areas outlined in UK government's CONTEST strategy, the congress will be opened by John Hayes MP, the UK's Minister for Security. As the person ultimately responsible for the country's counter-terrorism, security, serious organised crime and cyber-crime strategies, he will deliver a speech on extremism, border security and international counter terror strategy.

A total of 29 high ranking officials and academics will lead the congress, providing invaluable trends and information. The leading security professionals are set to discuss a variety of topics such as extremism, border security and the UK's international counter terror strategy. Covering current counter terror and security tactics, extremist propaganda, and the expansion of ISIS it is not to be missed.

Cyber security takes centre stage

Following the recent increase in cyber threats, Chancellor George Osborne pledged that the UK will spend £1.9bn over the next five years to deliver a series of initiatives to protect the economy and infrastructure, grow cyber companies, and deter adversaries.

Security & Counter Terror Expo will mirror these advances in the industry, showcasing cutting-edge technology and exploring the latest cyber security strategies at the free-to-attend Cyber Threat Intelligence Conference. Starting on April 19th, leading figures will discuss the latest solutions and strategies at the two-day conference. Presented by techUK, the representative body for the UK's technology industry, the sessions will bring together all those who work to prevent cyber terrorism and crime.

Among the topics to be discussed will be an overview of global cyber security threats and how to mitigate against them, protecting the "smart" critical infrastructure and overcoming the cyber security skills shortage.

Key speakers will include Chris Gibson, Director at CERT-UK; Richard Parris, Chairman and Chief Executive of Intercede; Prof. Chris Hankin, Director at the Institute for Security Science and Technology; and representatives from the National Crime Agency's National Cyber Crime Unit.

Talal Rajab, Programme Manager for techUK's Cyber, National Security and Criminal Justice programmes, added: "What was once considered a niche area in the wider national security debate has emerged front and centre in many government's priorities. Security & Counter Terror Expo offers the ideal platform for the industry to learn from some of the most prominent figures, while networking with key decision makers."

Protecting critical national infrastructure

In addition to safeguarding the digital frontier, security professionals are tasked with the protection of critical national infrastructure (CNI). Terrorist groups continue to not only threaten civilians, but also communications networks, the emergency services, energy plants, financial institutions, governments, health services, transport links and natural resources.

The Critical National Infrastructure & Business Reliance conference will aim to aid public and private entities to identify, assess, prioritise, and protect critical infrastructure and key resources. Allowing them to detect, prevent, deter, devalue, and mitigate deliberate efforts to destroy, incapacitate or exploit a nation's CNI.

The conference will feature a series of presentations examining the policy and strategy responses to today's terror threat. Leading figures will discuss the latest advances in the protection of critical national infrastructure in Europe, staff responses to extreme events and the impact on national infrastructure organisations and critical information infrastructure protection in financial services.

Providing invaluable insight and information, more than 20 high ranking officials and academics will feature during the conference. Representatives from the likes of the National Counter Terrorism Policing HQ, the Home Office Centre for Applied Science & Technology (CAST) and the Israeli Ministry of Transport will discuss a variety of topics. The lively and engaging sessions will focus on the latest advances in the protection of critical national infrastructure in Europe, staff responses to extreme events and the impact on national infrastructure organisations. The potential for UAVs in the protection of critical aviation infrastructure will also be covered.

Driving the transport security agenda

Running alongside the Critical National Infrastructure & Business Reliance and Cyber Threat Intelligence conference, the Transport Security Live will focus on discussing effective security solutions for the global transport infrastructure.

The global terror threat is high and transport networks are a favoured target. The free-to-attend Transport Security Live Conference will showcase international case studies and the latest developments in protecting transport networks, transport hubs and passengers.

The conference will bring together the key stakeholders from government, police, aviation, maritime, public transport, and rail to discover best practice, the latest solutions and developments in transport security. Comment on the importance of Peter Cook, Chief Executive Officer, of the Security Association for the Maritime Industry said: "Terrorists will stop at nothing to cause maximum damage and that includes targeting critical national and global infrastructure. Preventing these kinds of attacks has never been more essential especially as 90% of all global trade moves by sea. Events like Transport Security Live are critical as they bring together a diverse group of professionals to exchange ideas in the hope of creating a safer and smarter transport network for all".

Cook will be joined by the likes of Dvir Rubinshtein, Manager, Aviation Security Operation Centre, Israeli Ministry of Transport; Inspector Chris Boyle, Strategic Partnerships – Prevent, National Counter Terrorism Policing HQ; and Peter Cook, CEO, Security Association for Maritime Industry.

Witness cutting edge technology

Public and private sector buyers, influencers and government delegations from across the globe will be attending Security & Counter Terror Expo to explore how the latest technology will enhance their current and future security needs.

At Advanced Technologies Live, visitors will be able to see and hear more about the latest technologies and innovative solutions that the industry has to offer through a series of live demonstrations. Attendees can view latest innovations from the likes of Canon, The Defence Science and Technology Laboratory which is part of the Ministry of Defence, CEA and Sqaurehead Technologies

On the second day of the event, Security & Counter Terror Expo will collaborate with The UK Drone Show to showcase the latest drone technology for the first time in the show's history. Attendees will see live demonstrations by some of the UK's top drone operators and companies. Designed to showcase the very latest in aerial and terrestrial unmanned vehicles, this new area will allow greater flexibility for product demonstrations than ever before.

Richard Wright of the UK Drone Show said: "This is a very busy and exciting year for us, and the collaboration with Clarion's Defence & Security Division brings our experience of the UAV/drone industry to a sector that will see huge benefits from this rapidly developing technology".

David Thompson, Event Director, said: "The 2016 event is set to be the best yet. The calibre of speakers at this year's show highlights that Security & Counter Terror Expo is the place to be for security professionals from across the globe."

Security & Counter Terror Expo 2016 is co-located with Ambition – the EPRR Expo – and Forensics Europe Expo.

To register to attend or exhibit at the 2016 Security & Counter Terror Expo or for further information, please visit http://www.counterterrorexpo.com/

For more information please contact Storm Communications on 020 7240 2444 or SCTX@stormcom.co.uk

About Security & Counter Terror Expo

Security & Counter Terror Expo is the event for professionals from the public and private sectors tasked with protecting against terrorism and delivering effective security strategies. It comprises of a free-to-attend exhibition, workshops, demonstrations and a high-level paid for conference. It takes places at Olympia, London from 19 – 20 April 2016.

CYBER DEFENSE AWARDS 2016

CYBER DEFENSE AWARDS

TSC ADVANTAGE
Securing the Enterprise

Threat Vector Manager™ (TVM) & Enterprise Security Assessment (ESA)

"The Most Innovative Enterprise Security Solution for 2016" - CDM

CYREN

CYREN WebSecurity

"The Best Anti-Malware Solution for 2016" - CDM

CYBER DEFENSE AWARDS

CONTRAST SECURITY

Contrast Enterprise

"The Best of Breed in Application Security Solutions for 2016" - CDM

WAPPLES

WAPPLES

"The Hot Company in Web Application Security Solutions for 2016" - CDM

CYBER DEFENSE AWARDS

VARONIS

Varonis DatAdvantage

"The Most Innovative Insider Threat Detection Solution for 2016" - CDM

eclectic iq

EclecticIQ Threat Intelligence Platform

"The Leader in Threat Intelligence Solutions for 2016" - CDM

CYBER DEFENSE AWARDS

DARKTRACE

Enterprise Immune System

"The Editor's Choice for Enterprise Security Solutions for 2016" - CDM

CyberX

CyberX XSense Platform

"The Best ICS/SCADA Security Solution for 2016" - CDM

CYBER DEFENSE AWARDS

MyDiamo

MyDiamo

"The Editor's Choice in Data Leakage Prevention (DLP) Solutions for 2016" - CDM

VARONIS

Varonis DatAlert

"The Hot Company in User Behavior Analytics Solutions for 2016" - CDM

EXHIBIT IN 2016

SSS
Saudi Safety & Security
2016

Saudi Arabia's leading security, fire and safety exhibition

16 - 18 May 2016
Dhahran International Exhibitions Center,
Dammam,
Kingdom of Saudi Arabia



The SSS 2016 international exhibition will play host to innovative and pioneering technologies and products aimed at overcoming security, safety and fire issues. Saudi Arabia is now one of the world's fastest growing markets for security and safety solutions, making the SSS 2016 exhibition an ample opportunity for companies to network with private companies offering solutions in the fire, safety and security space.

> "A great launchpad for getting collaborators/prospects/potential clients in the Middle East region together. The perfect event for safety professionals."
>
> Neclilae Edcuard,
> Marketing Manager, Invictus (Adina SRL)

2015 PARTICIPANTS

Want to exhibit?

Please contact Mostapha Khalil E: mostapha@bme-global.com T: +44 203 463 1097

Previous Supporters

2015 Sponsors

Official CPD Member

Organised by

Official Production House

Official Housing Agent

2016 Media Partners

www.sss-arabia.com

Follow us on Twitter: @bmeevents
For all the latest news: @SSS_Arabia #SAUDISECURITY2016

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

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

VS.

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

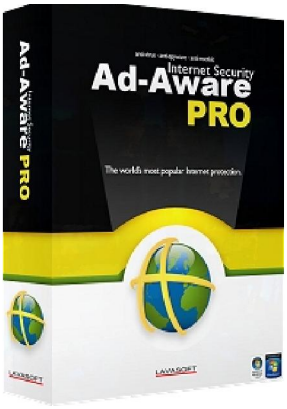
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting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

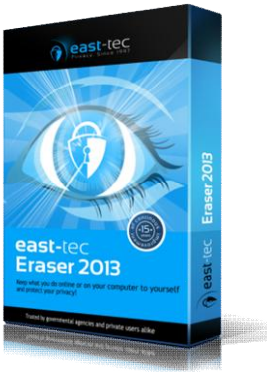
Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

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

SOURCES: CDM and NAISG.ORG

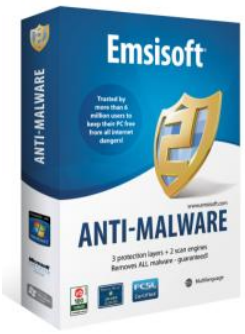




SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com

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



Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine March 2016

Sample Sponsors:

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

Cyber Warnings Newsflash for March 2016

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

MedStar Health's network shut down by malware

http://www.computerworld.com/article/3048959/security/medstar-healths-network-shut-down-by-malware.html

Malware scam appears to use GPS data to catch speeding Pennsylvania drivers

http://www.theverge.com/2016/3/27/11312960/speeding-ticket-malware-scam-email-pennsylvania

TreasureHunt PoS Malware Linked to Illegal Credit Card Sharing Forum

http://news.softpedia.com/news/treasurehunt-pos-malware-linked-to-illegal-credit-card-sharing-forum-502310.shtml

Attackers Use Multiple Digital Certificates For Malware To Thwart Detection

http://www.lifehacker.com.au/2016/03/attackers-use-multiple-digital-certificates-for-malware-to-thwart-detection/

Criminals abuse eBay-owned Gumtree.com.au to spread malware

http://www.cso.com.au/article/596849/criminals-abuse-ebay-owned-gumtree-com-au-spread-malware/

Stealthy malware targeting air-gapped PCs leaves no trace of infection

http://arstechnica.com/security/2016/03/stealthy-malware-targeting-air-gapped-pcs-leaves-no-trace-of-infection/

Unusual Data-Stealing Malware

http://www.informationsecuritybuzz.com/articles/eset-discovers-unusual-data-stealing-malware/

Beware unofficial apps: why Android malware won't go away

https://www.androidpit.com/beware-unofficial-apps-why-android-malware-will-not-go-away

Smooth Criminal: Meet USB Thief, A Malware That Can Attack Systems Without Leaving Any Trace

http://www.techtimes.com/articles/144306/20160326/smooth-criminal-meet-usb-thief-a-malware-that-can-attack-systems-without-leaving-any-trace.htm

Malware authors quickly adopt SHA-2 through stolen code-signing certificates

http://www.computerworld.com/article/3048346/security/malware-authors-quickly-adopt-sha-2-through-stolen-code-signing-certificates.html

EMAIL SCAM PETYA LOCKS DOWN PCS UNTIL A RANSOM IS PAID

http://www.digitaltrends.com/computing/petya-malware/

A third of email sent to U.S. House is malware, a virus or spam

http://www.usatoday.com/story/news/politics/2016/03/21/third-email-sent-us-house-malware-virus-spam/82078964/

Malware-infected Transmission 2.9 app threatened OS X users, stopped by XProtect

http://appleinsider.com/articles/16/03/06/malware-infected-transmission-29-app-threatened-os-x-users-stopped-by-xprotect

Malware used in $100 million Bangladesh bank heist

http://www.marketwatch.com/story/malware-used-in-100-million-bangladesh-bank-heist-2016-03-21

Opening a PDF on your iPhone could infect it with malware

https://www.grahamcluley.com/2016/03/opening-pdf-iphone-infect-malware-unless-youve-updated-ios-9-3/

Largely undetected Mac malware suggests disgraced HackingTeam has returned

http://arstechnica.com/security/2016/02/largely-undetected-mac-malware-suggests-disgraced-hackingteam-has-returned/

To bypass code-signing checks, malware gang steals lots of certificates

http://arstechnica.com/security/2016/03/to-bypass-code-signing-checks-malware-gang-steals-lots-of-certificates/

Malware Is Now Signed with Dual Certificates, for SHA1 and SHA2

http://news.softpedia.com/news/malware-is-now-signed-with-dual-certificates-for-sha1-and-sha2-502138.shtml

Attackers packing malware into PowerShell

http://www.theregister.co.uk/2016/03/15/attackers_packing_malware_into_powershell/

Be Careful. Mistyping a Website URL Could Expose You to Malware.

http://www.slate.com/blogs/future_tense/2016/03/17/hackers_use_om_urls_for_typosquatting_malware_attacks.html

Android Malware Leaves Mobile Banking Users Vulnerable

http://www.pymnts.com/news/mobile-payments/2016/android-malware-leaves-mobile-banking-users-vulnerable/

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

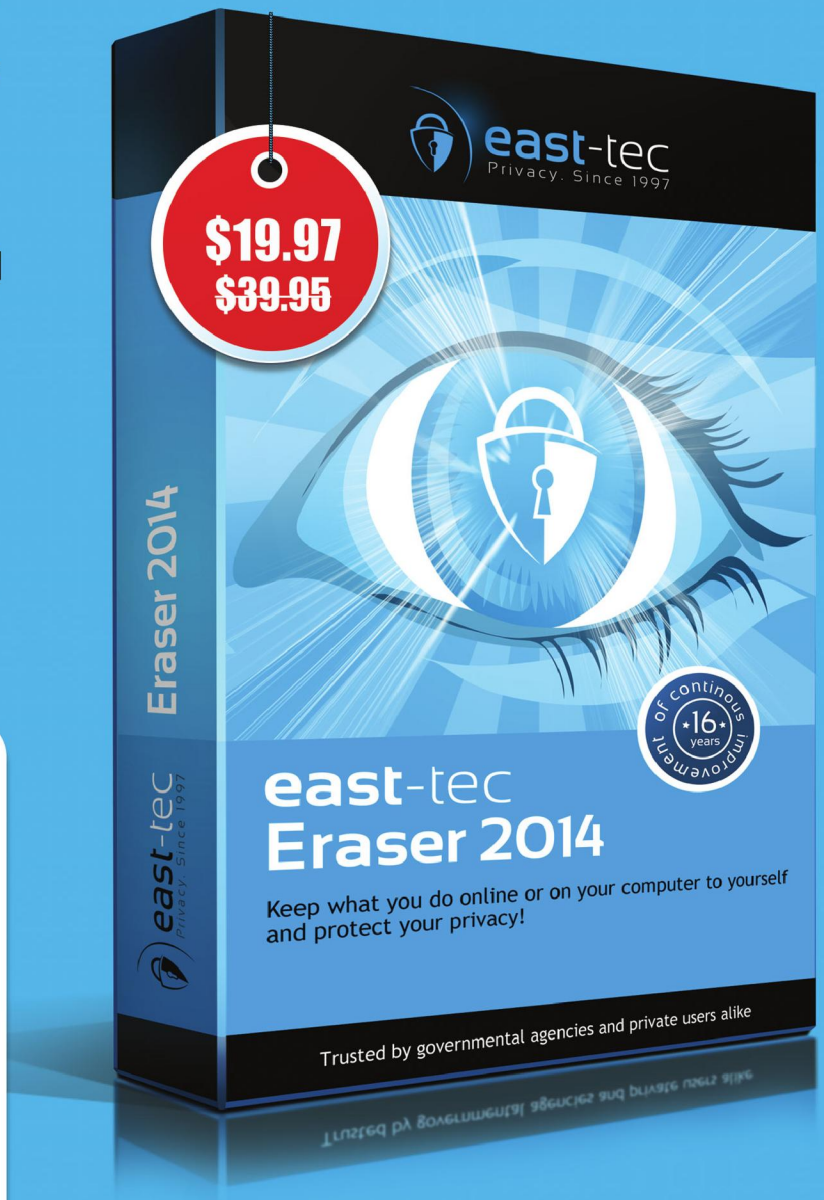
Cyber Defense Magazine - Cyber Warnings rev. date: 03/30/2016

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

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



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014

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