CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

NETWORK PERFORMANCE

CYBER SECURITY STRATEGIES

ENTERPRISE SECURITY

DEFCON & RECENT EVENTS

August 2014

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

Pierluigi Paganini
Manton Angus
Scott Robohn
Brandon Hoffman
Mike Raggo
Lorenzo De Leon
Milica Djekic
Zulfikar Ramzan
Julian Lovelock
Fred Touchette
Chris Coleman
Alan Kessler

and many more…

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Organizations Should Revisit Their Cybersecurity Strategies

Cyber Defense begins with understanding your risks. The risk formula is simple: Risks = Threats x Vulnerabilities x Assets or R = T x V x A. You cannot quantify cyber risks when you are unaware of the threats to your organization, the vulnerabilities in your network and computing equipment and all of the devices allowed to come and go on your network. More than 70% of organizations today have BYOD, or Bring Your Own Device, policies that allow employees to use mobile devices for both business and personal use. These devices are powerful enough to support corporate applications - and advanced malware. IT Directors should have stringent policies for personal devices being used for work applications to prevent attacks and data leakages. An enterprise level command center or dashboard is the way ahead in administering policies and rules.

Another major item left unnoticed and neglected are network maps. With increasing network complexity and outdated network maps, security holes are inevitable. It is important to close all paths to important and valuable data.

Multi-factor authentication techniques should be deployed to minimize the risk of intrusions and data thefts. It is also the single best method to provide secure access to employees from remote locations and also helps meet compliance requirements.

If you can quantify the risks to your organization (and start to include people – their devices, their behavior, the data they are allowed to roam with), then you can begin to bolster your cyber defenses. Take a closer look at this risk formula and start to find the weak spots. Start now before you are exploited and the risk of a major attack causing massive damage will be circumvented because you were one step ahead of the next threat. If an asset doesn't belong on your network, you should know if you OWN the entire network topology map. If an asset has a vulnerability you should know BEFORE it gets exploited. If there is a major threat exploiting that vulnerability you should bolster defenses until you can patch or remediate. Know your risk formula and be proactive!

To our faithful readers, Enjoy

Pierluigi Paganini

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

P.S. Congrats Olivia (USA) – this month's contest winner!

An Insight Into The Security Risks While You Engage In Social Networking Activities

Social networking has become the order of the day. Sites like Facebook, LinkedIn and micro blogging sites like Twitter have taken over the world of communication via the internet.

These sites are extremely popular among the young and old alike and the efficacy of these sites cannot be overemphasized. There are many uses for such sites. They can be used for making new friends and also for discovering old ones. They can be instrumental in finding employment and also for searching suitable candidates. Sites like Twitter can help one voice one's concerns and express thoughts and ideas on an international platform. Companies can increase their revenue and reach an astounding number of people through these social networking activities.

With the several advantages also come some very serious concerns. We share many things about ourselves on these sites. Personal information that we share while signing up is stored within the servers of these websites. Of the three websites that have been mentioned in this article, Facebook is the one that is used the most by a staggering number of people worldwide. Facebook users share their status, photos and communicate with their 'friends' on a regular basis. We may have seen status messages that look very simple but they may have serious repercussions.

Imagine a Facebook user posting a status message that says, ''Yippee, Going on a week-long Caribbean cruise vacation with entire family on Friday''. It is a very innocent message that expresses the person's joy and excitement. But the message that it conveys is very potent. For her friends it may sound fun but there are people who may observe it in a different way. They now know that the person will be away from home for a week. The house will be empty for one full week starting from Friday. Would you get on the rooftop and shout out the same things to the world? If you won't then don't do so on Facebook or any other social networking site.

Recently there was a questionnaire that was forwarded by many on Facebook. It included a series of questions that would supposedly be used to judge a person's character. Some of the questions also asked for the name of the person's elementary school and the user's mother's maiden name, name of first pet and so on.

Now pause for a moment and think where else you may have seen the same questions. Got it? Exactly, while opening an online bank account, or for your work's HR system you are required to answer a series of questions that will help you retrieve your password if you forget it. It may be very harmless between friends but there are hackers who could get hold of this information and drain your bank account without you even knowing it.

There are many applications on Facebook that are designed by end users. These may be in the form of calendars and questionnaires. You will have to download and install these applications or add them as 'add-ons' to your browser. These applications may contain malicious content that could copy your passwords or usernames.

Twitter is another popular micro blogging site. People tend to post all kinds of personal information as well as their opinions on various things. If a software architect working in a reputed firm tweets ‘’Just found out a major bug in ‘Decipher 1.01’, Wonder who screwed up ☹’’, he is doing a major disservice to the firm that he works in. In some cases employees have even been fired for having inadvertently leaked sensitive company information.

Social networking sites play a very important part in bringing people together and as mentioned before their importance cannot be overstated. But there are many security risks in social networking that needs to be dealt with. Make sure that your computer has antivirus/malware tracker software. Do not download any applications or software unless you feel they are absolutely necessary. Verify that they are from reputed sources.

Most importantly prevent these issues from happening. Do not post information that is sensitive or status updates that could be used by unethical characters. As a well-informed user you must be able to maintain security and also educate others on how to protect themselves as well.

About the author

I am **Manton Angus**. I focus on essay services reviews last a few years which have helped me out to gain knowledge in various disciplines of writing assignments for all class of students. I have worked with different essay writing companies as part of my profession and experiences bring lots of opportunities to write about more topics.

Network Performance Monitoring and Diagnostics (NPMD): Why DPI Is Essential

By Scott F. Robohn, Director Solutions Architecture and Engineering, Procera Networks

2014 marks the first year that Gartner has released a magic quadrant report for Network Performance Monitoring and Diagnostics (NPMD)[1] – a strong indicator of this market's increasing importance—valued at approximately $1 billion. The authors of this Gartner study note that the number of technologies and services that must be supported is constantly increasing. Multiple, new applications appear every day for mobile and desktop users and devices, along with the control protocols that run behind the scenes to make those applications work. New versions of these applications also roll out constantly which include changes in their behavior making them difficult to identify. We also expect increased use of automation as software-defined networking (SDN) and network functions virtualization (NFV) increases to grow in prevalence, feeding into the volume and complexity of the growing pool of available applications. [this sentence doesn't make sense]

As a result of the steady increase in applications and protocols the NPMD landscape will continue to become increasingly complex for the foreseeable future. Application identification via Deep Packet Inspection (DPI) is needed to address this rise in complexity so that NMPD tools can keep up with the ever-changing application landscape.

The NPMD market itself has evolved as a result of the increasing intricacy of today's networks. NPMD tools provide the ability to detect, identify, and prevent issues related to the many applications traversing the Internet and the networking devices and appliances that are the Internet's physical infrastructure. These tools drill down using various analytic and diagnostic applications to monitor the components in a network with the goal of reducing outages, providing troubleshooting information when incidents occur, and optimizing performance.

IT professionals have utilized a number of tools over the years to troubleshoot their networks, but these primitive, reactive solutions have lost their efficacy due to the network's evolution. To be useful in the modern environments, NPMD tools must now have built-in application intelligence to take a more proactive approach and to provide better identification of new apps as they appear in the network.

So how are NPMD tools advancing to meet these new requirements?

NPMD tools leverage three key technology areas to accomplish their objectives: SNMP polling, flow-based technologies, and packet-based technologies. SNMP polling was a useful first-generation element management technology, but it has significant limitations in that it requires explicit support of the SNMP protocol, SNMP polling itself can have an impact on resource utilization on managed network elements, and it was never designed to provide a detailed real-time view of application traffic. Flow-based technologies (NetFlow, Jflow, Sflow, IPFIX, and others) can provide more timely information, but they were designed to provide summary information, often taking a traffic sampling approach, and can also cause resource

utilization issues. Both SNMP and flow-based techniques lack the ability to provide granular application info, especially metadata about application flows, in real time.

DPI is an essential, packet-based technology that has evolved to enable NPMD solutions with real-time visibility into application traffic. To accurately classify and identify the complex mix of traffic flowing across the network, a combination of DPI classification techniques must be used to achieve the real-time visibility and accuracy required by NPMD tools.

Procera's embedded DPI engine – the Network Application Visibility Library (NAVL) – takes a data driven approach to identification of application traffic. It examines the packets of an application flow via a robust set of classification techniques to provide visibility in real-time by using: deep protocol dissection, behavioral analysis, future flow awareness and flow association, surgical pattern matching, conversation semantics, and deep protocol dissection. The Procera NAVL team also provides proactive coverage of new applications as they emerge, along with metadata from ongoing application flows. NAVL's combined use of these techniques provides the Layer 7, real-time visibility that NPMD solutions need with the rapidly increasing complexity of today's networks.

About the author

Scott Robohn is an IP networking professional with over 23 years of experience in Service Provider, Enterprise, and US Federal Government markets. He delivers solutions and technology expertise in large-scale IP/MPLS networking, including Network Function Virtualization (NFV), Mobility (3G/4G/LTE), SP Edge and Core, Data Center/Cloud, Software-Defined Networking (SDN), Network Security, and other areas. Prior to joining Procera Networks, Scott served in a variety of leadership roles at Cisco and Juniper Networks, leading teams of highly-experienced pre-sales architects and consulting engineers. Scott has also served as a Certified Cisco Systems Instructor (CCSI), an adjunct faculty member at George Mason University, a Network Architect at Bell Atlantic (Verizon), and a consultant to the Federal government on networking and security issues. Scott lives with his wife and children in Fairfax City, VA.

The Killer App for Security

Brandon Hoffman, Federal CTO, RedSeal Networks

Next Generation Threat Environment

Security has long felt like a losing game. As we know, the good guys need to be lucky all the time, but the bad guys only need to be lucky once. We have all spent vast amounts of money, time and effort trying to ensure the security of our sensitive information, and that of our customers. Firewalls, intrusion detection systems, SIEMs, anti-malware products, VPNs, vulnerability scanners – layer upon layer of defense. Yet, despite our best intentions, we now know that breaches are almost inevitable. The bad guys have gotten into our networks, and are lurking there, waiting to discover just one route to critical data that can be exfiltrated for personal, financial or political gain. We're all looking for that "killer app" for security.

Evolving Threats

The new class of threats looks quite different than threats of the past. We have seen threats move from casual hacks done for fun or glory, to financial attacks (by tapping into underground networks to sell credit card data), corporate/government espionage (e.g. the Night Dragon attack on multinational energy companies), weaponization of code (as hacktivists take revenge on those with whom they disagree), all the way to Advanced Persistent Threats such as Stuxnet and Operation Aurora. Many of today's bad actors are well-funded, well-equipped and well-versed in network architecture and human behavior.

The lifecycle of the advanced persistent threat is disturbing. Attackers select their target, and easily acquire the necessary tools on the Internet, purchasing information on vulnerabilities, renting botnets, etc. They then do recon on the infrastructure – and the employees (often through email and phishing attacks, but also increasingly via mobile devices), and begin their work. Initial probing quickly shows vulnerabilities that can be exploited for the initial intrusion. Once in, they build a command and control center with outbound connections. Then they stealthily work to increase their footprint, gathering credentials and learning about the network. Through persistence and patience, they find critical data and exfiltrate it. Quickly moving to cover their tracks, they wait patiently for the next opportunity to do it all over again.

Root Causes of Network Vulnerability

There are two principal causes of network vulnerability that can lead to breaches and loss of critical data: the ever-expanding attack surface, and increasing network complexity. While employees play a growing role in network vulnerability, the amount – and value – of data to be protected is growing even faster. All the while, attackers often have the financial backing and the patience to continue to bombard your network, seeking one small vulnerability that will let them in.

Expanding Attack Surface

How do attackers get in? Increasingly, it is via mobile devices. More than 70% of organizations today have BYOD, or Bring Your Own Device, policies that allow employees to use mobile devices for both business and personal use. These devices are powerful enough to support corporate applications - and advanced malware. The lines between personal and business use are blurred, and users consequently underestimate threats and introduce risk. In general, mobile security behavior is sloppy. A big back door just opened up into your network. The attackers no longer need to try to find the weakest link in your network security – they have it. Malware can be injected through social engineering attacks, downloaded apps and more: mobile messaging exploits and denial of service attacks are becoming commonplace. These can lead to unauthorized network connectivity, sensitive data leakage, and exfiltration.

Increasing Network Complexity

Network complexity is perhaps the biggest root cause. Today's networks are no longer simple, easy-to-understand and explainable in a Visio diagram. Rather, they have grown increasingly complex. Organic growth alone contributes to complexity, as newer systems and approaches are layered on top of existing systems. Even in a well-planned network, the loss of "tribal knowledge" due to employee turnover can quickly lead to major gaps in corporate understanding. And when you factor in mergers and acquisitions, the situation can rapidly spiral out of control.

Even the savviest IT team probably doesn't know exactly what the network looks like, much less how it is working. In many organizations, the most recent network map is at least five years old. Many of the devices currently in the network didn't even exist when the map was made. Out-of-date maps make it difficult to validate whether vitally important initiatives, such as secure enclaves or vaults, have been set up properly. But the task of updating the network map never rises to the top of the priority list.

Confronting Next Generation Threats

The task of securing critical information in this environment is not easy. The bad guys don't care about the cause of the vulnerability – they just need to get in, via the path of least resistance, and then explore: which people talk to which other people, what systems talk to what other systems, where does critical data (such as credit card data, personally-identifiable information, trade secrets) probably live? And from there, what are all the avenues that could be used to take critical data out?

It turns out the knowledge is the security "killer app" – in this world security is built on knowledge. Make sure your employees know the risks and responsibilities that come with mobile devices, and are trained to avoid social engineering attacks. Bear in mind that the path to increased user awareness is slow and bumpy. That's why it is imperative to constantly monitor and protect your network, since the threats can only be reduced but not eliminated.

Network knowledge is perhaps even more important. Know what normal behavior on your network looks like, so you can spot abnormal behavior. Know what your network itself really looks like, rather than working on an assumption or from a hopelessly out-of-date map. Know where your critical data resides, and all the paths that could lead an attacker to it. Know how you want to protect that data, and whether your efforts are actually resulting in the protection you desire.

The easiest way to build this knowledge is through visualization. For networks, the "killer app" takes the form of a network map. Mapping your network – and being able to know and see all the devices, where they are and what they can get to – allows you to do a form of triage. It quickly shows you all the paths to – and from – your most valuable data. It gives you a roadmap to fix them, in an iterative fashion. Once the most undesirable paths have been closed off, you can then repeat the process until you are certain that your most critical data is actually being protected the way you want. Mapping lets you see whether your secure enclaves are actually implemented as intended.

Conclusion

Threats are growing in sophistication, employing new and innovative ways to attack our strategically important networks. Knowledge: of the nature of the attacks, the attack surfaces used, and the reasons behind our continued vulnerability, is the "killer app" that will help us gain full visibility. Visibility leads to knowledge, and from there to power. It's our most effective weapon against an increasingly sophisticated bad actor who needs only a bit of good luck (or lack of knowledge on our part) to infiltrate, exploit and exfiltrate our most critical information.

About the author

Brandon Hoffman is a technology professional with more than 15 years of experience ranging from practitioner to management. Brandon's core experience is with information security and security program development/management, high availability (trading and broadcast) networks, wireless platforms, and data center. Prior to RedSeal, Brandon held roles at KPMG, Chicago Mercantile Exchange, Clear Channel, Bonneville Radio, and Boingo Wireless amongst others. To keep himself fresh, Brandon teaches an undergraduate EECS course and a graduate level information security course at Northwestern University in Chicago, IL.

Put Your File Transfers... Under LOCK & KEY

- SIMPLIFY
- AUTOMATE
- ENCRYPT

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

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

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

SEE FOR YOURSELF

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

Later, Vegas! Recapping Black Hat, Defcon and BSidesLV

Mobile Apps, App Wrapping, and Mobile Device Vulnerabilities Top of Mind at Security Conferences

By Mike Raggo, Security Evangelist, MobileIron

It is exciting to see the brightest minds in security and hacking descend on Las Vegas each summer for Black Hat and Defcon. In recent years, these shows have spawned offshoot conferences like BSidesLV that aim to leverage all that security muscle in one place. I was fortunate to be invited to participate at all three shows for the second year in a row and I wanted to share some of the biggest security takeaways.

To sum up information security learnings in a word, it would be "complex." With the unprecedented transformation we've seen in digital information gathering and the growing number of threat vectors, it's no longer enough to just focus on the big picture. Protecting data today requires a strategic plan that addresses both proactive and reactive countermeasures to ensure we're following best practices. We need to worry about the little things.

Black Hat reportedly had more than 8,000 attendees this year. The show typically grows in attendance year over year, as security researchers disclose their latest security vulnerability research to the world. Unbeknownst to some, Black Hat stemmed from the original security hacker conference known as Defcon, which now immediately follows Black Hat and just celebrated its 22nd year. Last but certainly not least is BSidesLV. The show has local conferences all over the U.S., but arguably their largest show is during the week of Black Hat Las Vegas.

Every year, security researchers seek to set the bar higher, and this year lived up to that reputation. In terms of mobile security, there were a number of notable presentations across the three conferences, so let's start out with the first conference of the week - BSidesLV 2014.

BSidesLV uncovered myths about mobile app security

BYOD and Mobile Devices more broadly have introduced a fundamental shift in the enterprise in terms of how people conduct business, increase efficiencies, and improve the customer and employee experiences. Mobile devices are inherently different from legacy PCs and laptops in that they represent a move from open operating systems to mobile operating systems that leverage application sandboxing, provide enhanced security management features, and empower the end-user.

But with this comes a new set of risks some of which stem from malicious or risky apps. The media has hyped the risk of malicious apps, but an annual report conducted by Appthority indicated that less than 0.4% of apps contained malicious behaviors, whereas roughly 81% of the mobile apps we use everyday contain a risky behavior that could arguably lead to data loss or exposure of PII information such as location, address, email address, phone number, and more.

I was fortunate to deliver a presentation with the President of Appthority, Domingo Guerra, titled "Bring your own Risky Apps". Domingo and I walked attendees through some freeware tools that allow organizations to review a mobile app and understand its behaviors. This enumerated that a wallpaper app was accessing location information, while other apps were harvesting the user's list of contacts and sending them to unknown adware sites. In an enterprise, this can be quite dangerous for obvious reasons.

We reviewed a variety of proactive and reactive countermeasures that identify all of the more than 2.5 million risky apps across the App Store and Google Play. We also discussed how enterprise mobility management (EMM) policy enforcement could be used to respond to a variety of threats by quarantining a mobile device when a malicious or risky app is identified.

This too represents a fundamental shift from PC-oriented anti-virus and anti-malware. In mobile, anti-virus and anti-malware is just another app. So while although it can detect malicious and risky behaviors, it's limited in what it can do in terms of removing the bad app because it's just another app on the mobile device and typically doesn't have the right to remove the threat.

Mobile App Risk Management solutions integrate with EMM/MDM solutions to leverage the ability to respond and mitigate threats.

Black Hat presentations put app data protection front and center

From the headline-grabbing auto hacks to the more than 100 briefings that touched on mobile vulnerabilities, it was obvious that an ever-growing ecosystem of endpoints present a clear and present danger to information security.

There were several briefings that stood out from a mobile security perspective. "Unwrapping the Truth: Analysis of Mobile Application Wrapping Solutions" focused on mobile application management (MAM) solutions leveraging a technology known as App Wrapping.

This involves taking an app and adding an additional layer of security code to the app to allow additional security controls to be applied through MDM/EMM policies. These controls can include strong authentication, encryption for data-at-rest, secure connectivity through application tunneling or per-App VPN, authorization controls, selective wipe, and more.

Presenters highlighted individual vulnerabilities found in a few EMM solutions including lack of encryption as well as exploits than can be performed on Jailbroken devices. At MobileIron, we authored a blog highlighting the presentation and security best practices in terms of countermeasures.

One notable countermeasure leverages jailbreak and root detection in conjunction with a quarantine if an attacker is trying to gain access to an application's data either at-rest or in-transit. It also reinforces the need for administrators to update their EMM products when updates are released as these updates sometimes include security patches.

Defcon reminds us to always update software

One presentation in the Wall of Sheep area of Defcon highlighted the recently publicized iOS Attachment Vulnerability. The vulnerability was discovered by Andreas Kurtz in April 2014 who revealed that iOS Data Protection (enabled by using a PIN or Passcode on your iOS device) was not protecting Mail Attachments.

This impacted iOS devices 7.1.1 and older. If an attacker booted one of these devices in Device Firmware Update (DFU) mode they could leverage a custom RAMdisk, and login over USBmux to read email attachments both from personal and corporate accounts in clear-text (no encryption).

Fortunately, EMM solutions with attachment security proved to offer protection from this threat. Attachment security encrypts corporate email attachments automatically. Apple has since released iOS 7.1.2 fixing this bug, so enterprises are encouraged to upgrade their iOS devices to the latest iOS release.

Top 6 takeaways

Three shows, 11 days, and thousands of attendees. These shows allowed the security community to come together, reveal cutting edge security research, and learn how to better fortify their networks. It was interesting to see that many of the mobile security themes from previous years are still prevalent:

1. Security is not a silver bullet. Employ a layered security approach to minimize single points of exposure.
2. Leverage encryption wherever possible both for data-at-rest and data-in-motion.
3. But Encryption alone doesn't protect data, so employ data loss prevention (DLP) as well.
4. Certificates can help. Man-in-the-Middle (MitM) attacks continue plague organizations, so ensure you're using certificates with SSL/TLS mutual authentications.
5. Be prepared. Ensure you have proactive and reactive countermeasures in place because, as they say, "it's not a matter of if, but when."
6. Patch it. Keep up with your security patches from vendors to avoid unnecessary threats.

Until next year, "may the force be with you".

About the author

Mike Raggo (CISSP, NSA-IAM, CCSI, ACE, CSI) is the Security Evangelist at MobileIron. He brings more than 20 years of security technology experience and evangelism to his role delivering mobile security solutions. Mike's technology experience includes mobile device security, penetration testing, wireless security assessments, compliance assessments, incident response and forensics, security research. He is also a former security trainer. In addition, Mike conducts ongoing, independent research on various data hiding techniques including steganography, Wireless and Mobile Device attack, and countermeasure techniques. His publications include books for Syngress titled "Data Hiding" and McGraw Hill as a contributing author for "Information Security the Complete Reference 2nd Edition", as well as multiple magazine and online articles. Mike has presented on various security topics at numerous conferences around the world (Black Hat, Defcon, SANS, Department of Defense Cyber Crime, Gartner, OWASP, InfoSec, etc.) and has even briefed the Pentagon and the FBI.

Mike Raggo can be reached online at @MikeRaggo and @DataHiding. Learn more about MobileIron at www.mobileiron.com.

Not All Two-Factor Authentication Techniques are Created Equal as Demonstrated by Emmental Attack

Voice channel two-factor authentication and transaction verification via secure data channel are protected from Man-in-the-Middle (MITM) and the SMS message-focused Emmental attack

By Lorenzo De Leon, VP of Applied Engineering at Authentify

All forms of two-factor authentication have not been defeated by the Emmental attack despite widespread reports to the contrary. In fact, it was the use of an SMS-delivered one-time password (OTP) that was exploited by the Emmental program cited last month in a Trend Micro report. The report detailed attacks on 34 Swiss, Swedish, Austrian and Japanese banks in which the exploit dubbed Emmental by Trend Micro allowed millions of dollars to be fraudulently wired out of legitimate accounts.

The researchers who uncovered Emmental indicate it is a variation of a man-in-the-middle (MITM) attack. Hackers send a targeted phishing email to an end user. The email appears to be from a popular retailer. The email has an attachment that when downloaded, installs malware on the user's computer. The malware then installs a rogue SSL root certificate which tricks the computer into trusting servers that look like those of their bank, but are instead controlled by the hackers. The malware then deletes itself to help avoid detection. The next time the user visits his bank website, they are routed to the fake banking website. The user will log in using their legitimate credentials, handing them to the hackers. The end user is instructed by the fake site to install a mobile app that will be used for additional security. Instead, the malicious app diverts the one-time passcode (OTP) the legitimate bank sends via SMS message to the end user's mobile phone for confirming unusual transactions. Armed with the user's login credentials and able to receive the confirmation OTPs, the hackers now have all the credentials needed to transfer funds to themselves.

The twist in this MITM variation is that it does include the redirect of an SMS message on the end user's mobile device via the malicious mobile app. The end user's ability to provide the correct OTP is the second authentication factor of the two-factor authentication schema for these banks.

Numerous MITM/phishing/malware attacks have demonstrated the vulnerability of SMS messaging for some time now. The twist in the Emmental variation is that it includes the redirect of an SMS message on the end user's mobile device via the malicious mobile app. As an authentication factor, SMS messages are still used due to their low cost, convenience, and ubiquity. End users are familiar with SMS messaging. The continued use of SMS despite the vulnerability is a risk vs. cost and convenience assessment a financial organization must make.

"It's disappointing that reports claiming simply that 'two-factor authentication has been beaten' are circulating once again when not all two-factor authentication techniques are of equal strength and other forms of two-factor have definitely not been beaten," said Alan Dundas, Vice President of Product for Authentify.

Dundas should know. As a former security architect at Symantec, he was responsible for authentication technologies that touched more than 1 billion end points globally. According to Dundas, “The problem lies with the practice of delivering a one-time password to the end user via SMS. In general, OTP approaches of this type were fine several years ago. They’re just not as secure as they once were. The cybercriminals have developed their own countermeasures.”

The Foundations of Two-Factor Authentication

Two-factor authentication is a practice in which a user provides more than one authentication credential. Traditionally, the first authentication factor used is “something you know,” or knowledge. This knowledge is normally a shared secret like a password paired with a username. Passwords are a valid shared secret when used appropriately. In many cases the convenience and security strength are appropriate for protecting free online accounts and other low value access points. In the case of financial accounts, however, a simple username and password combination is obviously far from sufficient.

Some institutions use a second authentication factor, but in the same “form factor” or category. A “something ‘else’ you know” as a second-factor of authentication is familiar to many. It could be a query for a mother’s maiden name or the make of the user’s first automobile. This factor could be formatted as multiple-choice challenge question. The idea is an end user would be able to answer a private and personal question easily while strangers would not. This technique is now inadequate due to the vast amount of personal information available across social media platforms as well as many other websites. Hackers are adept at capturing and mining this information in order to thwart knowledge based authentication.

Institutions that acknowledge this vulnerability and wish to increase security may migrate to an authentication factor that is “something you have.” An ATM card is an example of something a user possesses in addition to a PIN when using an ATM. A security token that delivers an OTP is also often used as a second authentication factor. The OTP received via token is then entered into the website. The rationale behind this method is that only the legitimate end user with ownership of this token will be able to receive the case-sensitive string of numbers to correctly connect and log in. Unfortunately, if the OTP is entered directly back into an infected Internet connection, the OTP is delivered to the hacker as well. That is the danger of a man-in-the-middle attack.

Passwords, usernames, transactional OTPs, and other information typed on the keyboard and delivered to a website are considered “in-band” communication. They may be delivered out-of-band, but they are then exchanged in-band, within the same communication band or channel in which the primary Internet connection exists. If a hacker or cybercriminal is monitoring that same channel via a MITM attack like Emmental, any confirmation information exchanged between the end user and the website will be compromised.

A Better Two-Factor Solution

Out-of-band authentication is the use of multiple networks or communication channels such as an internet connection and a telephony network, working simultaneously to authenticate a user. As has been shown with OTPs however, simply delivering an authentication token like an OTP out-of-band and then entering it in-band is not good enough. That communication

channel is compromised and the session itself is compromised. Details about the session itself must be provided to the end user via a second communication channel for the end user to recognize that something is wrong.

Typically the more security applied to a process the less convenient it becomes for the end user. This is especially true if the user is required to overcome a multi-step process simply to log in to an account. Especially in the light of the fact that exploits like Emmental are not thwarted by a strong login process. Depending on the circumstances, it may be a better user experience to apply authentication periodically throughout a user session instead of stacking it at the beginning.

Requiring end user authentication of "post-login" activity, especially activity that affects the account or transfer of funds, is one solution to these problems as well as threats similar to Emmental.

For instance, an institution that is equipped with telephone-based, out-of-band authentication services can employ those services for transaction verification vs. simply login authentication. The end user can receive a telephone call that repeats transaction details for approval. For end users equipped with smartphones or tablets, an encrypted messaging channel to an app might be employed to deliver transaction details for approval instead of SMS.

Thinking outside the box, applying additional authentication measures "post-login" need not be related to only transactional verification. Imagine a process in which the end user uses a smart device that scans a QR code as the last task before they log out to finalize changes to the account. Behind the scenes, the QR code scan triggers a digital certificate authentication. The user interface is clean and easy and products of this type are available today. End users, after all, are familiar with signing letters, tax returns, and other documents as the last part of a process. An end user will accept additional authentication layers more readily provided they are streamlined and applied when a user already has invested some time in account activity that is sensible to protect.

There are additional benefits when requiring out-of-band authentication for opening new accounts or when making changes to existing accounts. Hackers often open multiple accounts for one institution in order to move funds around and appear legitimate before making a fraudulent transfer. An institution utilizing this technique adds a little friction to the account registration process for a fraudster. A legitimate user will provide a phone number readily. The fraudster establishing a single telephone number to many accounts relationship is providing a data point that can be flagged as a risk point for examination. The fraudsters can acquire multiple phones, but the extra work may simply cause them to go after an easier target.

As described above, the ability to tailor an authentication process to counter different threats at different points in the end user's workflow is requisite for successfully thwarting modern cyber-thieves. When considering authentication technologies an institution should have the flexibility to choose which, how many, where and at what times authentication factors are used to authenticate an online user or their activities. By layering authentication or verification at natural points in the user's workflow an institution will still be able to provide an

intuitive and convenient user experience as well as a much higher level of safety in an increasingly perilous online environment.

About The Author

Lorenzo De Leon is the VP of Applied Engineering at Authentify Inc. Lorenzo has over 20 years

About Authentify, Inc.

Authentify provides multi-layered, device-based user authentication services that can be controlled by enterprise policy, while offering a very simple, intuitive and consistent end user experience. Its solutions protect more than a trillion dollars in transaction value with device-based authentication worldwide. Customers include the top three e-commerce sites, five of the world's largest banks and the top four insurance companies. Inc. Magazine has ranked Authentify among America's fastest growing private companies.

For more information, visit Authentify at: www.authentify.com

Authentify's technologies are protected by multiple U.S. and International patents.

Stuxnet: The Revolutionary New Cyber Weapon

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

As modern cyber attacks are getting more complex and sophisticated, our world is suffering a serious deficit in an adequate security tool or software capable of detecting such an advanced threat. The problem with the new generation of malware is that they can easily break into every system, but stay undetected there for a long period of time. In this article, we attempt to explain in brief the new cyber weapon bringing the revolutionary approach to modern cyber warfare and military affairs. Its name is Stuxnet and right now it's the one of the best known advanced malware for doing sabotage in the world.

Introduction

In June, 2010 Stuxnet malware has been identified by a small Belarusian software firm while it came to spread an infection through some USB stick. But, that's not all. The majority of infection has occurred in Iran within their nuclear plant at Natanz which was the part of their nuclear program. Luckily, this cyber division delayed the development of Iranian nuclear weapon by more than 4 years. It has been speculated that this malicious worm is the secret project of some scientific team from the US and Israel. However, Stuxnet has done its job by getting over 100,000 machines in the world infected.

Stuxnet is the next generation sophisticated malware which purpose is a sabotage of the industrial equipment. Some sources claim that Stuxnet entered an Iranian nuclear complex on some removable device, probably USB stick. Once it makes a system infected, it starts working on the sabotage of industrial controllers. It can affect some sorts of PLC (Programmable Logic Controller) equipment within an industrial plant or, in Iranian case, within a nuclear complex. This malware spreads very fast through network and after some period of time it begins to do a sabotage. In general, it would accelerate the centrifuges controlled by PLCs and cause the complete malfunction of the industrial equipment.

The crucial issue with such a threat is it cannot be easily detected using the modern ways of malicious software detection. These can be pretty concerning since the equipment can get malfunctioned and no one will get what caused that. The main concern is that Stuxnet is just the beginning in advanced threats development. Hackers are always one step ahead security. The new versions of modern and improved malware are coming and they are threat for everyone in this world, so some measures should be taken in order to prevent from such attacks.

How Does Stuxnet Work?

Stuxnet was designed to cause a failure to industrial equipment. It is designed for sabotage, not crime. Its aim is a, so called, SCADA (Supervisory Control and Data Acquisition) system. This system serves in controlling of critical infrastructure such as industrial equipment, power plants and so on. The Stuxnet worm can get into SCADA systems very easily through the

Internet, local area network or very often through some removable device. It is not necessarily needed to have a network connection and Stuxnet will get to some PLC.

How is this possible? Well, as it is normal to do some PLC programming, you must use a computer (usually with Windows platform) with an adequate PLC developer's tool. A PLC, by itself, can operate even if it is disconnected from the network, once its governing software has been transferred into its processor's system. As it is known, some updates should be done regularly even through network connections or through removable devices and that's how a PLC's software can get infected. The interesting thing is worm causes the minimal harm to a PC computer and makes a great damage only to PLCs that have some centrifuges attached to them. This is feasible because the worm can detect if there is some frequency converter attached to PLC as the link between a controller and a rotating part of the industrial machine.

What is also interesting in Stuxnet's case is that it attacks only some sorts of Siemens PLCs and it is suitable for 32-bit Windows only. This is the fact because the majority of targeted infrastructures use an equipment with those characteristics. It is obvious that some insider's information about the situation within the industrial plans existed before the development process of Stuxnet warm has begun. It seems that the project Stuxnet has been carefully and strategically prepared. That's why this cyber warfare operations were that successful.

Stuxnet Invalidates Some Security Assumptions

Stuxnet invalidates several security assumptions. Let us see how! The first such assumption is that *isolated systems are more secure*. We were talking about this, bit is' not definitely case with this worm. As it is known, SCADA systems control mission critical machinery, many administrators do not connect these computers to a network – attempting to achieve security by isolation. As a result, you need to update your system somehow. You will do that through file transfer to such machines which is conducted by removable media. The designers of Stuxnet exploited this assumption by enabling the worm to spread through the memory sticks. That allows a system to get infected even if it's not connected to the network.

Another key security assumption Stuxnet invalidates is *the trust relationship set in place by digitally-signed certificates*. In order to provide more stability, modern operating systems, including Microsoft Windows, limit a computer program's access to system components. A normal program requests systems calls to hardware via driver software. As such is the case, the driver software has more access to lower-level system components than other programs. To avoid the easy creation of malicious driver software, Microsoft Windows relies on digitally signed certificates. In order to prevent detection by anti-virus software, Stuxnet uses legitimate digitally-signed certificates. In other words, this worm will set the trust relationship in place by digitally-signed certificates that it already uses. The computer's platform will see this malicious software as a trusted application.

Conclusion

This article is an attempt of the simple and comprehensive review of this very interesting malware solutions. As it is known, malware and threats are coming from very skillful and motivated teams which work for governments, academia, industry or hacker's community. Stuxnet is a great example of the next generation highly sophisticated threat which is expected to progress and get improved. It is also a good example of the next generation cyber weapon capable of doing more harm than a standard military operation. The similar software are also a serious threat to modern world, so, above all, this sorts of advanced malware should be seen as one of the biggest challenges for security nowadays.

About The Author

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

CYBER SECURITY SUMMIT 2014

Connecting C-Suite Executives With The Leading Cyber Solution Providers

June 5, 2014 • DC Metro
September 18, 2014 • New York City

The Cyber Security Summit provides a forum for executives to learn about the latest in cyber security protection by connecting them with world-class solution providers, expert speakers and powerful decision makers. **Cyber companies interested in joining us, please contac**

Ken Fuller, Executive Vice President
(212) 655-4505 ext. 234 / KFuller@TechExpoUSA.com

Senior Executives: $250 (50% off with promocode CDM2014)
Government Executives: $50
Event Details & Tickets: CyberSummitUSA.com

Sponsored By:
THE WALL STREET JOURNAL.

A Special Thanks To Our 2013 Summit Sponsors

McAfee • FireEye • PwC - PricewaterhouseCoopers • F5 Networks • RSA, The Security Division of EMC • PhishMe
Blue Coat Systems • AirWatch • Brite Computers • BUMI (Back Up My Info) • CipherPoint Software • Mocana
NIKSUN • National Cyber Security Alliance • Cognizant • Dickstein Shapiro LLP • eSentire • Savvis Federal Systems
Guardian Data Destruction • Guidepoint Security • Hewlett Packard • HillCrest Agency • Websense • Triumfant
Information Security Solutions • Information Systems Security Association (NY) • LifeLock • Lookingglass
NetCom Learning • Norman Shark • Norse • Novetta Solutions • nPulse Technologies • Prevalent Networks
Red Sky Alliance • Reservoir Labs • Security Innovation Security Innovation Network (SINET) • Skybox Security
STIGroup • ThreatGRID • ThreatTrack Security • Vir-Sec • Vistage • ZenSar Technologies • Ziften • Zscaler

CyberSummitUSA.com

How Organizations are Rethinking Their Cybersecurity Strategy

The Three Habits of Smart Organizations

by Zulfikar Ramzan, Ph.D., Chief Technology Officer, Elastica, Inc.

It seems like new words are unceasingly creeping into the IT lexicon: Cloud, BYOD, Internet of Things, and so on. While these technologies are a veritable goldmine from the perspective of gaining new organizational efficiencies, they are simultaneously a minefield from the perspective of IT security.

Each of these technologies can materially impact an organization's risk posture and significant thought is required to bring them into the fold in a safe and sane manner. To make matters worse, organizations are also dealing with far more insidious attackers. Gone are they days when online miscreants would send victims typo-ridden emails in broken pseudo-English offering a million dollars tomorrow in exchange for a far modest payment today. These low-budget kitchen sink campaigns have been replaced with carefully honed social engineering operatives designed to dupe even highly sophisticated users in far more insidious ways. It's the difference between a smash and grab robbery at a 7-11 and an Ocean's Eleven type of heist.

When I look at how Chief Information Security Officers (CISOs) at major organizations are rethinking their cybersecurity strategy in the face of these issues, a number of common themes seem to be emerging.

The first common theme is that smart organizations think about cybersecurity from the perspective of the full threat lifecycle. Consider, for example, the Adaptive Security Architecture framework developed by Neil MacDonald and Peter Firstbrook of Gartner. This framework comprises four key elements: prediction, prevention, detection, and response.

Prediction is about being able to establish a baseline regarding where you are today from a security perspective. What are the most significant vulnerabilities in your environment and what are risks you need to be concerned with? It's important to start outlining your security strategy by considering risks before you consider threats. After all, a threat is merely something that takes advantage of an existing risk. Technologies like vulnerability scanning and vulnerability assessment are commonly used here.

Prevention is about being able to stop threats before they infiltrate your environment. Technologies for providing access control and policy enforcement come into play here. More so, if you think about it, about twenty years ago, network security was almost entirely focused on technologies for prevention, like the firewall.

Detection is about identifying threats that actively present themselves into your environment. You can detect threats by looking for known patterns (often termed "signatures") or by trying to infer the intent behind a broader set of behaviors using more sophisticated analysis. The underlying techniques notwithstanding, the bulk of enterprise security focus nowadays is centered on detection. However, it's becoming clear that detection is no longer sufficient as

wily attackers routinely bypass even the detection capabilities that well meaning IT security organizations have in place today.

Therefore, smart organizations are also considering response as part of their overall strategy. Here you begin by capitulating that attackers will get through. Next, rather than asking yourself "what if?", you ask "now what?" instead. Incident response is about determining the scope, ramifications, and ultimately the root cause associated with the threats your organization is facing. One critical capability along these lines involves continuous monitoring. Keep track of relevant information as it comes in, and when you need to piece together what happened after the fact, it's far simpler.

To make a physical analogy, it's like having a security camera in place. These cameras might not do much in the way of preventing crime, but they are invaluable in allowing you to determine what actually happened. Questions that previously required hours of painstaking expert forensic analysis can be answered by looking at a few minutes of camera footage.

Organizations today are putting these "cameras" in place across their IT assets: networks, endpoints, and traffic going to and from cloud services. Not only do they save time in doing so, but they can take whatever lessons they've learned and re-apply them back to the prediction phase, thereby coming full circle. These capabilities are simply indispensible in today's world.

The second common theme is that smart enterprises are coming to the realization that security is fundamentally about data science. All of the elements discussed above involve gathering, processing, gleaning insights from, and acting on data. Therefore, organizations are thinking about how they can take whatever technologies they have in place today, and make them work as part of a common data analytics fabric.

This type of thinking is certainly not without its challenges. After all, organizations still have to deal with a tremendous amount of legacy infrastructure and legacy processes. Consequently, no solution will be without its faults. At the same time, smart organizations are realizing that they need to make strategically sound decisions moving forward so that security becomes less about point solutions and whack-a-mole, and instead becomes far more comprehensive and holistic.

The third common theme is that smart organizations do not just focus on technology, but rather strive towards engendering a culture that values information security from the executive ranks to the rank and file. Without this type of culture in place, it will be difficult to make long term progress. And because cybersecurity is highly dynamic, we simply cannot expect today's measures to work equally well tomorrow. Attackers are constantly adapting their methods, so we must constantly adapt as well.

Attackers aren't haphazard in their efforts. Therefore, organizations too cannot be haphazard in their response. Rather than implementing a series of quick fixes and praying for the best, you need to make holistic changes so that you are more than adequately prepared to deal with the worst head on.

About the author

Zulfikar Ramzan is the Chief Technology Officer of Elastica, the leader in Data Science Powered Cloud Application Security (http://elastica.net). In this role, he drives Elastica's efforts in leveraging data science and machine learning techniques towards improving the security of cloud services.

Prior to joining Elastica, Zulfikar was Chief Scientist at Sourcefire (acquired by Cisco), within their cloud technology group. At Sourcefire/Cisco, he was responsible for the technical vision as well as the in-field efficacy of the company's core advanced malware protection offerings. Prior to joining Sourcefire via its acquisition of Immunet in 2010, Zulfikar was Technical Director of Symantec's Security Technology and Response division. In all of these roles, Zulfikar used expertise in machine learning, large-scale data mining, and information security to protect customers from threats to their data.

Zulfikar has co-authored 50+ technical articles, and two books including Crimeware: Understanding New Attacks and Defenses, Addison-Wesley Professional, 2008. Zulfikar has 50+ patent applications, 40+ of which have been granted. He was selected and served as General Chair of Crypto 2010, the premier conference in the field of Cryptography. Beyond that, Zulfikar is a frequent public speaker and has briefed both numerous media outlets including the New York Times, Wall Street Journal, Associated Press, and Reuters as well as members of the United States Congress on cyber-security trends and issues. Zulfikar has produced a series of cybersecurity educational videos (sourcefire.com/chalktalks) and has also served as a guest faculty for the educational non-profit Khan Academy (khanacademy.org).

Zulfikar holds a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology, with thesis work in cryptography.

Extending the Benefits of Strong Authentication Across the Enterprise

By Julian Lovelock, Vice President of Product Marketing, Identity Assurance, HID Global

Enterprises have typically focused on securing the network perimeter and relied on static passwords to authenticate users inside the firewall. This is insufficient given the nature of today's Advanced Persistent Threats (APTs) and internal risks associated with Bring Your Own Device (BYOD) adoption. Since static passwords can be a potential recipe for a security disaster, enterprises would benefit from not only employing strong authentication for remote access, but also extending its use to cover the desktop, key applications, servers, and cloud-based systems as part of a multi-layered security strategy.

Unfortunately, choosing an effective strong authentication solution for enterprise data protection has traditionally been difficult. Available solutions have been inadequate either in their security capabilities, or in the user experience they deliver, or in the cost and complexity to deploy them. Now, we have the opportunity to eliminate these problems using Near Field Communications (NFC)-enabled credentials that can reside on smart cards or smartphones, and can be employed to secure access to everything from doors, to data, to the cloud. Versatile, NFC-based strong authentication solutions can:

Support converged secure logical access to the network and cloud-based services and resources, as well as physical access to buildings, offices and other areas;

Support mobile security tokens for the most convenient and secure access from smartphones or tablets; and

Deliver multifactor authentication capabilities for the most effective threat protection, as part of a multi-layered security strategy.

The Challenges of Strong Authentication

Multi-factor authentication, also known as strong authentication, combines something the user knows (such as a password) with something the user has (such as mobile and web tokens), and can also be extended to include a third factor in the form of something the user is (which can be ascertained through a biometric or behavior-metric solution).

Users have grown weary of the inconvenience of hardware OTPs, display cards and other physical devices for two-factor authentication. Additionally, OTPs are useful only for a limited range of applications. The industry is now replacing hardware OTPs with software tokens that can be held on such user devices as mobile phones, tablets, and browser-based tokens. With software OTPs, organizations are able to replace a dedicated security token with the user's smartphone, enabling the two-factor authentication to grow in popularity and convenience. A phone app generates an OTP, or OTPs are sent to the phone via SMS. However, there are security vulnerabilities with software OTPs that have driven the need for a far more secure strong authentication alternative, such as smart cards based on the Public Key Infrastructure (PKI). The downside to this approach, however, is its high cost and level of complexity to deploy.

Future Mobile Opportunities

The benefits of NFC technology are many as it becomes a standard feature of smart phones, tablets and laptops targeted at the enterprise market. Users can have a smart card or smartphone that grants access to resources by simply "tapping in" – without the need to enter a password on touch-screen devices, or the need for additional devices to issue and manage. In addition, there are a number of steadily growing NFC-based tap-in use cases that are poised for strong adoption in the enterprise, including tap-in to facilities, VPNs, wireless networks, corporate Intranets, cloud- and web-based applications, and SSO clients, among many other scenarios. These benefits and the wide range of potential applications – along with the fact that manufacturers are enabling more and more phones, tablets and laptops with NFC -- are driving many companies to seriously consider incorporating secure NFC-based physical and logical access into their facilities and IT access strategies.

The mobile model will deliver particularly robust security, and will be especially attractive in a BYOD environment. It will be implemented within a trusted boundary, and use a secure communications channel for transferring identity information between validated phones, their secure elements (SEs), and other secure media and devices. The authentication credential will be stored on the mobile device's secure element, and a cloud-based identity provisioning model will eliminate the risk of credential copying while making it easier to issue temporary credentials, cancel lost or stolen credentials, and monitor and modify security parameters when required. It will also be possible to combine mobile tokens with cloud app single-sign-on capabilities, blending classic two-factor authentication with streamlined access to multiple cloud apps on a single device that users rarely lose or forget.

The NFC tap-in strong authentication model will not only eliminate the problems of earlier solutions, it will also offer the opportunity to achieve true convergence through a single solution that can be used to access IT resources while also enabling many other applications. These include such physical access control applications as time-and-attendance, secure-print-management, cashless vending, building automation, and biometric templates for additional factors of authentication – all delivered on the same smart card or NFC-enabled phone alongside OTPs, eliminating the need to carry additional tokens or devices. Historically, physical and logical access control functions were mutually exclusive within an organization, and each was managed by different groups. Now, however, the lines between these groups will begin to blur.

Additional Considerations for the Cloud

As identity management moves to the cloud and enterprises take advantage of the Software as a Service (SaaS) model, there are other critical elements to consider. For instance, it will be critical to resolve challenges around provisioning and revoking user identities across multiple cloud-based applications, while also enabling secure, hassle-free user login to those applications.

The most effective approach for addressing data moving to the cloud will likely be federated identity management, which allows users to access multiple applications by authenticating to a central portal. It also will be critical to ensure the personal privacy of BYOD users, while protecting the integrity of enterprise data and resources. Several other security issues also emerge. IT departments won't have the same level of control over BYODs or the potentially

untrustworthy personal apps they may carry, and aren't likely to be loading a standard image onto BYODs with anti-virus and other protective software. Nor is it likely that organizations will be able to retrieve devices when employees leave. We will need to find new and innovative ways to address these and other challenges. Notwithstanding the risks, the use of mobile phones equipped with SEs, or equivalent protected containers, opens opportunities for powerful new authentication models that leverage the phone as a secure portable credential store, enabling use cases ranging from tap-in strong authentication for remote data access, to entering a building or apartment.

Additionally, as BYOD continues to grow in popularity and many cloud-based applications are accessed from personal devices, enterprises will need to take a layered approach to security, recognizing that no single authentication method is going to address the multiple devices and multiple use cases required by today's mobile enterprise.

A Layered Security Approach

In addition to multi-factor user authentication as the first layer of security, both inside the firewall and in the cloud, there are four other layers that should be implemented.

The second layer is device authentication. In other words, once it is determined that the user is who he or she says she is, it is important to verify that the person is using a "known" device. For this step, it is important to combine endpoint device identification and profiling with such elements as proxy detection and geo-location.

The third layer is ensuring that the user's browser is part of a secure communication channel. Browser protection can be implemented through simple passive malware detection, but this does not result in the strongest possible endpoint security. It is more effective to use a proactive hardened browser with mutual secure socket layer connection to the application.

The fourth layer is transaction authentication/pattern-based intelligence, which increases security for particularly sensitive transactions. A transaction authentication layer can include Out-Of-Band (OOB) transaction verification, transaction signing for non-repudiation, transaction monitoring, and behavioral analysis.

The final layer is application security, which protects applications on mobile devices that are used to deliver sensitive information. The application must be architecturally hardened and capable of executing mutual authentication. Adding this layer makes data theft much more complex and costly for hackers.

Effectively implementing these five security layers requires an integrated versatile authentication platform with real-time threat detection capabilities. Used in online banking and ecommerce for some time, threat detection technology is expected to cross over into the corporate sector as a way to provide an additional layer of security for remote access use cases such as VPNs or Virtual Desktops.

Migrating to New Capabilities

Migration to NFC-based strong authentication and true converged solutions requires an extensible and adaptable multi-technology smart card and reader platform. For optimal flexibility and interoperability, this platform should be based on open architecture, and enable both legacy credential and new credential technology to be combined on the same card while also supporting NFC-enabled mobile platforms. To meet security requirements, the platform should use contactless high frequency smart card technology that features mutual authentication and cryptographic protection mechanisms with secret keys, and employs a secure messaging protocol that is delivered on a trust-based communication platform within a secure ecosystem of interoperable products.

With these capabilities, organizations can ensure the highest level of security, convenience, and interoperability on either cards or phones, along with the adaptability to meet tomorrow's requirements including a combination of both strong authentication for protecting the data and applications in the cloud, and contactless high-frequency smart card capabilities for diverse physical access control applications.

With proper planning, organizations can solve the strong authentication challenge while extending their solutions to protect everything from the cloud and desktop to the door. These converged solutions reduce deployment and operational costs by enabling organizations to leverage their existing physical access control credential investment to seamlessly add logical access control for network log-on. The result is a fully interoperable, multi-layered security solution across company networks, systems and facilities.

About the author

Julian Lovelock, **Vice President of Product Marketing, ActivIdentity, part of HID Global**

Julian Lovelock is the vice president of Product Marketing of ActivIdentity, part of HID Global, and is responsible for defining and bringing to market products across the Identity Assurance portfolio. Mr. Lovelock is based in Fremont California, having relocated from London in 2006. He joined ActivIdentity in 2005 as part of the acquisition of ASPACE Solutions where he was CTO and co-founder. Since joining ActivIdentity he has held a number of positions in product management as well as market responsibility for ActivIdentity's security solutions for online banking. Lovelock holds a BENG in Electrical and Electronic Engineering from the University of Aston, UK.

Is it gameover for Zeus?

By Fred Touchette, AppRiver

The Zeus family of malware has been around for quite some time now, since 2007 to be exact. The ever-changing strain has been focused on stealing bank account credentials from those who have been unlucky enough to fall victim to its bait.

In the very beginning, Zeus was sold as a malware kit on underground forums for several thousands of dollars with various plugins offered as add-ons for a la carte pricing. This went on for years as Zeus dominated the malware scene. But eventually, varying forms of Zeus' code began to appear online for free and it wasn't long before amateur cybercriminals compiled their own versions of the ubiquitous strain.

Frustrated with the freely-available rogue versions of his software, Zeus creator, SpyEye, threw in the towel and stopped supporting his creation altogether. But that didn't prevent Zeus-like malware from spreading and infecting thousands of users. Now in the hands of cybercriminal groups, the malware leaked around the globe by way of botnet (many, many botnets). It was only a short time after that a new variant called 'Gameover Zeus' or 'GOZ' hit the interwebs.

Gameover Zeus was operated by a single group located in Russia and Ukraine. The malware had new capabilities and operated using a peer-to-peer communication architecture that made it difficult for White Hats to pin down. An infected bot, for example, simply relied on another infected bot for instructions. And since bots were not communicating with a main command and control server, it became increasingly difficult to track and conquer. Gameover Zeus was ultimately responsible for the download and installation of malicious payloads that include the now infamous piece of ransomware known as CryptoLocker as well as other downloaders such as PonyLoader, Jolly Roger, BeeBone and Pushdo known for adding bots to the Cutwail botnet.

Operation Tovar

The group responsible for Gameover Zeus enjoyed Internet freedom for quite some time. But in June 2014, several foreign countries banded together with the U.S. Department of Justice, the FBI, the U.K. National Crime Agency and Europol who then also teamed up with security and academic researchers to fight the malware. By working together, these groups were able to take down a highly-aggressive botnet, which allowed Internet users to enjoy a collective sigh of relief - even if the relief was short lived.

1-Up

In July 2014, we started to see a new form of life stirring from what we thought was a departed botnet. Fake e-statements hit email inboxes that claimed to be from a company called 'Cards OnLine,' and in typical fashion these emails had an attachment that looked like

a PDF which urged readers to look inside at “their account information.” Instead, the attachment contained a Trojan compliments of Gameover Zeus.

Interestingly, it looks like the Gameover Zeus group abandoned its once effective peer-to-peer communications protocol and instead opted for a more direct command and control architecture that hides behind a domain name-generating algorithm to receive orders from its C & C. It also appears that the malware has changed the way it maintains a foothold in an infected host. But underneath the surface there are undeniable trademark signs that Gameover Zeus is back for more.

At this time, it is unclear whether or not Gameover Zeus is back with a vengeance or simply making that one last dramatic gasp for air as it continues to descend back into the depths of a deep, dark web. But one thing’s for sure, all eyes are on this botnet to see what it could possibly have in store for us next.

How to Stay Safe

In order to protect yourself from the remnants of Gameover Zeus, CryptoLocker and most other Internet threats, it is important to monitor your online actions and never become complacent in day to day activities.

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

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

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

About the Author

Fred Touchette, CCNA, GSEC, GREM, GPEN, Security+, is a Senior Security Analyst at AppRiver. Touchette is primarily responsible for evaluating security controls and identifying potential risks. He provides advice, research support, project management services, and information security expertise to assist in designing security solutions for new and existing applications.

Navigating the Threat Intelligence Hype

By Chris Coleman, CEO, Lookingglass

Having returned from Black Hat USA 2014 it has become apparent that threat intelligence is nearing the cusp of the hype cycle. As with any potentially disruptive method, the ability for those interested in sorting through the chaff to understand the root benefit becomes extremely difficult. In the spirit of transparency, I want to disclose up front that I have the privilege of being at the helm of a for profit business in the cyber threat intelligence market. My career path has afforded me exposure to this potential disruptive method for over a decade.

Let me first explain why I refer to it as a method. The promise of threat intelligence in of itself is not to be realized through technology alone, but by the method in which it becomes implemented and adopted within the overall security operations process.

In order for an organization to be able to use threat intelligence they must first realize that intelligence is derived by humans, and that an internal competency is required to effectively convert information into organizationally relevant intelligence. At that point, and only that point can the information be leveraged to create a dynamic security and risk posture.

So competency requires a plan, repeatable processes and procedures that can operationalize the information set, deemed in this case, and for lack of a better term threat intelligence.

While technology can provide a keen advantage to assisting in the collection, processing, analysis and enablement of the information, it will require a competency reliant on people and organizational processes and procedures to realize the benefit of this disruptive capability.

Why does threat intelligence have the potential to be disruptive? While there may be many different answers abound, my answer is that it is the first step in expanding our nearsighted approach that we've been taking for so long. Security has been focused at and within the perimeter. As a profession we have failed to extend our viewpoint to where 95% of the threat originates – outside the perimeter.

Experts speak of kill chains, yet only through threat intelligence can we get in front of the kill chain - adapting our security and risk posture based on threat information we receive. This information may not spell out a traditional "to do" list. Rather, it requires a competency to derive the telltale signs most important to your organization.

What kind of information makes up this threat-centric view? Another topic rich with opinions; however, if we can agree that what we're trying to achieve is a better informed security and risk capability, then there needs to be a strong focus on understanding the unknown. Understanding the unknown requires diverse information sets that when coalesced can help drive decision support on how to react. Ultimately, we are trying to increase the mean time to know; therefore, dramatically reducing the effect or preventing it all together.

Additionally, the faster we can get ahead or identify the threat, the more pain we put back on the attacker. It forces them to change, and reestablish infrastructure. Finished intelligence reports, while valuable, have already come to a predetermination or established a known quantitative result from a specific tactic, technique and procedure. In the time it takes for this information to be validated, vetted, decomposed and released, the adversary has already achieved some degree of their objective.

To take advantage of threat intelligence an organization needs to develop a competency and complimentary technology set that drives efficiency and effectiveness in taking atomic threat indicators and rapidly reducing, and or hardening the attack surface and overall potential impact based on the risk these indicators present.

This approach still leverages more finished products like human verified and vetted threat intelligence and threat research; however, threat intelligence must provide a tipping and cueing mechanism that attempts to move at the speed of the constantly evolving and fluid threat landscape. To move and adapt at that speed, requires us to accept that we won't always have the detailed answers, or at least not immediately. Using these varying and at times loose, but telling information sets can truly move us from a reactive posture into a more adaptive and dynamic posture.

The challenge with indicators as a threat information source is that they are numerous and change rapidly. Therefore, we need the industry to adapt the technology sets used to protect and defend our networks and assets. These technology sets will need to be updated in near real-time and support extremely large enforcement policies that change at an unprecedented frequency. So as any industry we must develop a competency to understand what this next generation of devices need to support.

What may have been presented as a high-risk element, signaled by an indicator, may no longer be in use by the time you even process the original indicator. This dynamic nature requires many different technology-driven mechanisms to handle the confidence of the indicator, but there also must be organizational competency to assess what the information is reporting and to determine whether that indicator poses a current or historical risk.

Even if the indicator is no longer of high confidence, understanding the timeframe in which it did pose a threat and whether an enterprise asset communicated with that entity is crucial information. So intelligence is not just a forward leaning capability, but one that can have great historical value. Our own internal incident response data can be coupled with these external indicators for an even more relevant and responsive information set.

As the threat intelligence market matures, there will be many more losers than winners. The legacy security players are being given another chance to retool their technologies of the past and provide more intelligence centric capabilities.

As an organization looking to leverage threat intelligence, remember that your people are the intelligence creators. Machines can provide the critical information that you need to know about the outside threat landscape to convert that information into relevant organizational intelligence to better adapt and defend your organization.

About the author

Chris Coleman, Chief Executive Officer

Coleman brings over 20 years of experience in information security and technology and a strong balance of hands-on experience and business acumen to his role as Chief Executive Officer at Lookingglass. He oversees all facets of the company's growth and direction, including delivery of products and services to Lookingglass' customers across the commercial, federal civilian agency and defense department communities.

Prior to Lookingglass, Coleman served as the Director of Cyber Security at Cisco Systems, Inc. where he focused on identifying solutions to critical customer challenges through delivery of Cisco and partner technologies for civilian, defense and intelligence organizations. Previously, Coleman served in key management roles with Integrated Data Systems and ManTech. During his tenure at ManTech, he was responsible for the remote security monitoring services and data hosting services profit and loss centers and managed ManTech's IT services and operations.

Coleman also managed the NetWitness product development team and was essential in the successful spin out of the technology and development team in 2006. Coleman studied Electrical Engineering at the New York Institute of Technology – Old Westbury. He is an active member of the cyber security community and enjoys ice hockey and skiing.

The Cybersecurity Battleground

Preparing for the War against Insider Threats

By Alan Kessler, CEO, Vormetric

You know that bad hacker movie, in which a company's credentials were compromised because a disgruntled employee clicked on a link with dancing cats? This just isn't reality. In fact, recent reports from Ovum and ESG found that both American and European organizations reported "privileged users," those being admins and network specialists, posing the biggest threat because their compromised accounts can cause the most destruction. The result may not be as severe as Snowden's revelations, but recent evidence proves that privileged users are as dangerous as traditional malicious insiders and can expose companies to data breaches, financial loss and reputational harm.

There is no rulebook that will tell us how insiders will behave

The number of insiders with credentials who can view and modify data across corporate networks (i.e. contractors, system engineers, network administrators and ordinary users) has exploded. When abused, these access credentials can be used as a way for insiders to infiltrate lucrative corporate networks. In the case of external attacks, this is often done with such stealth that infiltration goes undiscovered for long periods of time, it's no wonder that so many people seem daunted at the prospect of managing this multi-faceted risk.

This year has seen example after example of damaging cyber-attacks against large organizations, sophisticated threats that bypass traditional security defenses and leverage compromised insider credentials. While not the most complex attack, the Target data breach remains anchored in top headlines and over a year after of Snowden's first revelations, NSA officials have told the press that his haul may have been as large as 1.7 million documents. While these security incidents vary in terms of scale and impact, they all highlight that organizations are continuing to fight and are attempting to defend from threats that lie within.

Good news: There's a silver lining,

Though the perimeter provides a necessary starting point in today's world of increasingly diverse and complex threats, a vital way to defend critical assets as threats begin to target the real treasure troves within organizations – the server – is to take a data centric approach to security. This involves implementing encryption and access policies to limit exposure, and monitoring access to identify anomalous user activity.

Let's look at our options

Though over half of respondents to the recent Ovum report said their biggest concern is every day users, CISOs are currently spending as much as 80 percent of their security budgets on perimeter and end point defense. When it comes to limiting insider threats most organizations tend to believe that enhancing their existing network defenses and end point protections are the best ways to approach the problem, but reports from Mandiant and Verizon this year highlight that these defenses are being bypassed by today's attacks.

The best way to safeguard and protect data inside these permeable perimeters is to add a data-centric approach – adding the security controls to protect data where it resides. This entails:

Protecting data with encryption and limiting access to those who need it when they need it

Logging and monitoring who, what, when and where data is accessed and then analyzing the information to spot potential compromises

This doesn't mean you can forget about keeping your network and end point security at a state of basic readiness. That would be like unlocking the doors and windows to your house when you are away. But it does mean that emphasis and investments in IT security software implementations needs to shift to data-centric protection.

Beyond your traditional enterprise perimeter, you also need to recognize that SaaS, big data and cloud environments are now a reality – and that adjustments need to be made to safeguard data used in these environments. Again, the solution is the same. Since your perimeter has now "ballooned" out to include external applications and environments not inside of your perimeter, take a data-centric approach to protecting your organization from threats in these environments. In fact, data-centric security can enable organizations to make full use of cloud and big data environments – taking advantage of the efficiency, cost-effectiveness and business advantages they offer.

Strategy needs to be adapted to meet these changing circumstances.

When choosing solutions to these problems, selection should hinge on a few critical points:

Coverage: Should address as many use cases as possible with a single platform across your entire IT environment, including; OS platforms, data centers, big data implementations and cloud environments

Scalability: Make sure security solutions can scale, and encrypt without affecting application performance

Simplicity: Implementation should be simple, easily implemented and managed as well as capable of integration with existing security, deployment and management tools

Conclusion

Organizations need to do more to deal with insider threats that range from employee and contractor misuse, to targeted and malicious APT threats. They are often hindered by the tendency to keep doing what worked in the past – to continue with security solutions that were deployed with the assumption that by protecting networks and endpoints, valuable data assets are safe. Rather than maintaining the status quo, organizations should change focus to add data-centric security to the mix (encryption, access controls and data access monitoring/analysis).

In the past, integrating these elements into an existing IT infrastructure was not synonymous with "easy" or "low impact." Encryption was viewed as intrusive and difficult to implement.

Fortunately, the technology is now simple to deploy and manage. With recent developments that leverage the hardware encryption capabilities of today's CPUs, it also has minimal impact on performance. Access control has also created thorny problems in the past, with traditional solutions making it nearly impossible for system maintenance, backup and other management tasks to continue without radical changes in operation. Implemented correctly, encryption with access control solves these problems – by never decrypting data except for authorized users and programs, system level tasks can complete without potential exposure of data. Monitoring and analyzing data access is a newer problem – but can be addressed straightforwardly by collecting data access information from encryption and access control solutions and analyzing data using a security information and event management (SIEM) solution or big data for security implementation.

Instead of being viewed as expensive, intrusive and complex, data-centric security should be looked at as a catalyst enabling business, government and educational institutions alike to achieve their internal objectives, reduce risks and meet the needs of customers. There's no excuse for unprotected data, regardless of where it lies. Remember when it comes to data security, it's always easy to ignore insider threats until someone gets hurt.

About the author

Alan Kessler joined the company in 2012 because he firmly believes that Vormetric has the potential to become the frontrunner in the data security industry. As CEO, Kessler is further accelerating Vormetric's business momentum by expanding the company's global footprint, targeting untapped market opportunities, achieving operational excellence, and extending Vormetric's leadership position in helping enterprises mitigate business risk across physical, virtual and cloud environments. Kessler has a proven track record of directing global corporate strategy and operations for security, enterprise software and storage systems leaders such as HP, TippingPoint (a division of 3Com), Attune Systems and Palm, Inc. Kessler holds a bachelor's degree in business from San Jose State University and an MBA from the University of California, Berkeley. Alan can be reached online at @kessalan and at our company website http://www.vormetric.com/.

Put Your File Transfers... Under LOCK & KEY

- SIMPLIFY
- AUTOMATE
- ENCRYPT

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

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

Visit GoAnywhere.com for a free trial.

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by LINOMA SOFTWARE

SEE FOR YOURSELF

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

155 Black hat hackers fail to crack Secure Channels' patented encryption technology

155 Hackers took the "Can You Break This" Challenge; None Could Break Secure Channels' New PKMS2 Patented Encryption Technology

By Richard Blech

Each year, Black Hat introduces the latest security technologies and brings with it of some of the best hackers in the world. With the masses of hackers in attendance, Secure Channels' wanted to do something a little different and introduce a "Can You Break This" challenge to any hacker that thought they could break our newly patented PKMS2 (Pattern Key Multi Segment, Multi Standard) Encryption Technology. Who doesn't like a little competition and the potential to win a new BMW? With any competition there can only be one winner and the results of this challenge produced a shutout. One hundred and fifty-five hackers participated, yet none were successful.

More than 75 percent of the 155 hackers did attempt to crack a secret encrypted file that held a virtual key to a 2014 BMW. As an innovator in the development of patented encryption technologies that protect data in motion and data at rest, we were confident that it was unbreakable. As the clock clicked down to the end of the conference at 5 pm on August 7, there were a lot of tired fingers and frustrated minds, but no one had cracked the code.

Data breaches do not just reside at the perimeter as the most serious breaches come unsuspectingly from within. Encryption protects your data with certainty by enveloping it with impenetrable encryption which leaves the thief (either internal or external) with only useless bits and bytes.

AES 256 has an NSA backdoor which means that an exploit already exists. What we need now is an encryption standard that truly has no backdoors. If the NSA has probable cause then they can obtain a warrant to get the data, but in other situations data should be protected to the point of impenetrability.

The Secure Channels' PKMS2 technology uses available FIPS-certified third party encryption libraries to produce "unbreakable" communications and data files through:

The usage of third party libraries enabling the process to be extensible to any future development in encryption patterns. Secure transmission and storage of data in a network or via mobile devices.

Breaking a file into segments and encrypts each segment individually while encrypting data and increasing the time to encrypt and decrypt a file by only 20 percent from AES 256 standard. PKMS2's strength rises exponentially with the number of keys used and patterns chosen.

The protocol/password used per segment is based on a pattern key and can be as simple or complex as necessary for authentication. An entire data file of any type (a photo, a song, a video, or a document) can be a password depending on what the user wants.

Every day we hear about the latest attacks and hacks, it's imperative that as a security community we are developing not only solutions that can mitigate today's threats, but are prepared for the next decade of attacks. We encourage other security companies to put their solutions to battle against the best test and hackers to ensure we are one step ahead of the bad guys.

About The Author

Richard Blech is CEO of Secure Channels Inc., a new cyber-security firm that creates robust, and state-of-the-art patented encryption technologies under exclusive license from Secure Channels SA that are compatible with every type of data available on the market. www.securechannels.com.

Organized By: INTELLIGENCE-SEC

CYBER INTELLIGENCE EUROPE 2014

22ND – 24TH SEPTEMBER 2014 - BRUSSELS, BELGIUM

Sponsors and Exhibitors:

EXCLUSIVE NETWORKS

Esteemed Speaker Line-up:

- **Jamie Shea,** Deputy Assistant Secretary General, Emerging Security Challenges, **NATO**
- **Troels Oerting**, Assistant Director – Head of European Cybercrime Centre (EC3), **EUROPOL**
- **Heli Tiirmaa-Klaar,** Cyber Security Policy Advisor, **European External Action Service (EEAS)**
- **Frederick Vanneste,** Director, Cybersquad, **Ministry of Finance, Belgium**
- **Wolfgang Roehrig,** Programme Manager & Project Officer Cyber Defence**, European Defence Agency (EDA)**
- **Eugen Valeriu Popa,** Counsellor, **Ministry of Regional Development and Public Administration, Romania**
- **Frans Kolkman,** National Cybercrime Program, **Dutch Police Force**
- **Milos Mijomanovic,** Digital Crime Officer, Digital Crime Investigative Support Sub-Directorate, **INTERPOL**
- **Udo Kroon,** Chief Information Officer, **FIU.NET**
- **Francesca Bosco,** Project Officer, **United Nations Interregional Crime and Justice Research Institute (UNICRI)**
- **Eirik Troones Hansen,** Prosecutor, Cybercrime section, **National Criminal Investigation Service, Norway**

Benefits of Attending:

- ✓ Analyse the latest threats to government computer systems in Europe
- ✓ Discuss the need to share information to protect national critical infrastructures
- ✓ Understand the issues being faced by European law enforcement agencies at tracing an attack
- ✓ Review how we can improve prosecution against cyber criminals who leak valuable information
- ✓ See the latest cyber defence solutions available from the private sector
- ✓ Network with 100+ attendees from the public and private sector who work in the cyber security domain

Interactive Workshop Details:

Project DENSEK – Joining forces against cyber threats on European level

22nd September 2014

10:00 – 14.15

Workshop Leader:

Bert Heerbaart, Program Director, **DENSEK**

Hosted by:

DENSEK

For more information visit – www.intelligence-sec.com

Book your place by:

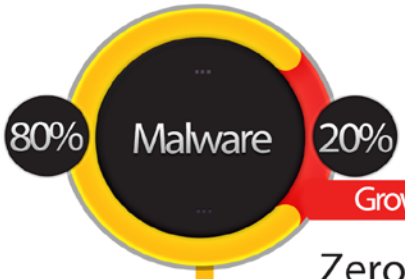
Web: www.intelligence-sec.com I Email: events@intelligence-sec.com I Tel: +44(0)1582 346706

SnoopWall

RECLAIM YOUR PRIVACY ™

TRADITIONAL MALWARE

Virus
Blended-Threat
Botnet
Zombie
Worm
Spyware
Trojan



MODERN MALWARE

Growing by 30,000 New Samples Daily

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

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

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

Get SnoopWall for

Windows (COMING SOON!)

iPhone (COMING SOON!)

Android

DID YOU KNOW ?

Less spying means longer battery life for your devices!

RECLAIM YOUR PRIVACY ™

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

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

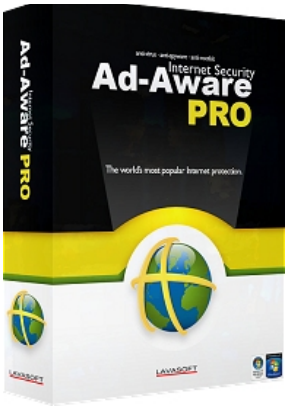
So use it by going here:

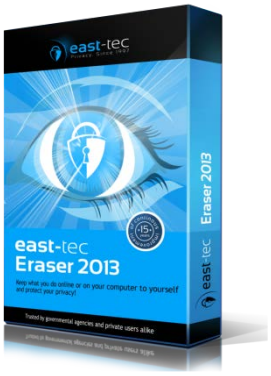
http://www.naisg.org/techtips.asp

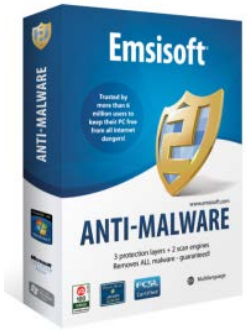
SOURCES: CDM and NAISG.ORG

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

http://register.cyberdefensemagazine.com







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

Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine August 2014

Sample Sponsors:

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

Cyber Warnings Newsflash for August 2014

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

Retailers warned of attacks using hard-to-spot PoS malware

08/01/2014 06:43 (Help Net Security)

Retailers warned of attacks using hard-to-spot PoS **malware** Retailers, beware: cyber crooks are increasingly targeting remote desktop applications...

Yes, Hackers Could Build an iPhone Botnet—Thanks to Windows

08/01/2014 06:38 (Wired)

...owners: Just because iOS has never been the victim of a widespread **malware** outbreak doesn t mean mass A reminder to Apple and smug iPhone owners:

CIA admits spying on Senate intelligence panel

08/01/2014 00:00 (Pittsburgh Post-Gazette)

...CIA never intended to give to Congress. In response, CIA **security** officials penetrated a secure **computer** server set up to allow the Senate investigators...

Malicious USB device firmware the next big infection vector?

07/31/2014 12:06 (Help Net Security)

...have created a whole new class of attacks that can **compromise computer** systems via Researchers from German **security** consultancy SR Labs have...

NSA keeps low profile at hacker conventions despite past appearances

07/31/2014 07:00 (The Guardian)

...mingled in recent years with some of the world s elite engineers and **digital security** experts at Black Hat and Def Con, Admiral Mike Rogers and...

China says Canada must 'stop making baseless accusations'

07/31/2014 05:00 (CTV News)

IAI refutes claim that Iron Dome makers were hacked

07/30/2014 19:22 (JPost)

...hackers looking for cheap technology steal, says former head of missile **defense** Uzi Rubin. Israel Aerospace Industries disproved reports by a US-based...

Connected vehicle cybersecurity: Opportunity and responsibility

08/04/2014 09:00 (The Hill - Blogs)

...an Information Sharing and Analysis Center (ISAC) to address the **cyber security** threat, similar to those created by the energy, financial services...

Bits and bytes in intelligence: Umbrella from OpenDNS

08/04/2014 08:01 (SC Magazine)

...us determine if addresses and domains are hosting attacks, malware or **phishing**. As one might expect, gathering that type of information needs...

Getting on Military Bases Is About to Involve FBI Background Checks

08/04/2014 07:24 (Nextgov)

...Henderson said in an email on Friday. IMESA will be operational on **Air Force**, Army, Marine, and Defense Logistics Agency installations that day,

Hacker says to show passenger jets at risk of cyber attack

08/04/2014 03:00 (Reuters US News)

Hacker says to show passenger jets at risk of **cyber attack** BOSTON Aug 4 (Reuters) - Cybersecurity researcher Ruben Santamarta says he has figured...

How secure are today's critical networks?

08/04/2014 02:13 (Help Net Security)

...on component failure probabilities, a quantitative model and measurements for **cyber security** levels do not exist. As a compromise, security certifications...

Army names a new general to head Cyber Center at Fort Gordon ahead of big expansion

08/03/2014 07:01 (Pendleton Times-Post)

...list) Subjects: Armed forces (310) Military and defense (830) **Government** and We also have more stories about: (click the phrases to see a list)

Updated NIST Guide Provides Computer Security Assessment Procedures for Core Security Controls

08/02/2014 09:27 (Technology News)

Updated NIST Guide Provides **Computer Security** Assessment Procedures for Core **Security** Controls (Targeted News Service Via Acquire Media NewsEdge)

The World's Most Hackable Cars

08/02/2014 08:30 (Dark Reading)

those two are on the same network, he says. Worries over the **cyber security** of cars is gaining traction ever since Miller and Valasek's 2013...

Cybercom Chief: Cyberspace operations key to future warfare

08/02/2014 00:10 (North Texas e-News)

Army Sgt. 1st Class Michael Deblock, Vermont Army National Guard **Computer** Network **Defense** Team, left, discusses new ways to make the exercise...

PittyTiger spearphishing campaign speaks multiple languages

08/01/2014 12:49 (SC Magazine)

...English. FireEye has observed the attackers using a Yahoo! email **phishing** pages kit that boasts **phishing** pages in different languages and aimed at...

Hackers 'constantly probing' federal computers: spy chief

08/01/2014 12:19 (CTV News)

Attackers can easily create dangerous file-encrypting malware, new threat suggests

08/01/2014 05:30 (Network World)

Attackers can easily create dangerous file-encrypting **malware**, new threat suggests A new program that encrypts files to extort money from users...

Invisible Web Infection Poses Threat to Federal Computer

08/05/2014 09:23 (Nextgov)

...say. Media networks were almost four times as likely to attract **malware** as the average enterprise network, likely because of an increasingly popular...

Tool Aims to Help Thwart Cyber-Attacks

08/05/2014 08:09 (GovInfoSecurity)

...information from the Internet to give organizations an early warning of a pending **cyber**-**attack**. The system, known as BlackForest, scrapes and analyzes...

Visit the Wrong Website, and the FBI Could End Up in Your Computer

08/05/2014 07:00 (Wired)

Visit the Wrong Website, and the FBI Could End Up in Your **Computer Security** experts call it a drive-by download : a hacker infiltrates a high-traffic...

Android RAT impersonates Kaspersky Mobile Security

08/05/2014 06:41 (Help Net Security)

...theft of cash from your account, please promptly install Kaspersky Mobile **Security** Antivirus on your **mobile device**," it urges, and apparently...

Google defends child porn tip-offs to police

08/05/2014 02:53 (Yahoo! News)

...caught," blogged John Hawes, chief of operations at Virus Bulletin, a **cyber security** consultancy. "However, there will of course be some who see it...

How to recognise the cyber insider threat

08/05/2014 00:11 (Computerworld Malaysia)

How to recognise the cyber **insider threat** If people start accessing systems or the data in them more often, you may have a problem. If people...

How Malware Writers Cheat AV Zero-Day Detection

08/04/2014 15:20 (Dark Reading)

How **Malware** Writers Cheat AV Zero-Day Detection A researcher reverse engineers AVG's code emulation engine after easily bypassing other major...

Cyber Security Challenge UK competition seeks sleuths to crack encrypted hard drive

08/04/2014 14:51 (Sophos Blog)

Cyber Security Challenge UK competition seeks sleuths to crack encrypted hard drive Sophos is calling on members of the UK public to turn cyber...

Stealthy malware 'Poweliks' resides only in system registry

08/04/2014 07:47 (Computerworld)

Stealthy **malware** 'Poweliks' resides only in system registry The **malware** is persistent across system reboots, despite not having any files on...

Chrysler, Nissan looking into claims their cars 'most hackable'

08/06/2014 09:13 (CNBC)

Chrysler and Nissan said they are reviewing a report by well-known **cyber security** experts that rates their vehicles among the three "most hackable"

Russian Gang ‘CyberVor’ Steals More than 1 Billion Passwords

08/06/2014 08:50 (CruxialCIO)

...through various means, including purchasing them from other hackers, from **malware** they implanted on users devices, and from botnets. While the...

State of security: malicious sites, CryptoLocker copycats, email scams

08/06/2014 08:33 (Help Net Security)

...Report, a detailed analysis of web and email-borne threats and **malware** trends tracked AppRiver released its mid-year Global Security Report, a...

Data Breach Bulletin: Credit Card Breach Confirmed At 33 P.F. Chang's Locations

08/06/2014 08:18 (Forbes.com)

...air defense against missiles, it hasn t proved safe from **cyber** attacks. Chinese **hackers** allegedly stole huge quantities of sensitive documents...

Payment cards used on Wireless Emporium website compromised by malware

08/05/2014 16:59 (SC Magazine)

Payment cards used on Wireless Emporium website compromised by **malware** After **malware** was discovered on the www.wirelessemporium.comcomputer...

A Peek at a Program That Lets Hackers Steal Anything From Your Smartphone

08/05/2014 16:14 (Bloomberg)

...software that steals banking passwords and text-message security codes. The **malware** even connects many of the devices with each other in a crude,

The Tech War On Child Porn Is Not Limited To Google Scanning Gmail

08/05/2014 15:49 (Forbes.com)

...sites hosted by a Nebraska man, the FBI turned his servers into a **malware**-delivery system so that anyone who sent a private message on his sites...

How Google handles child pornography in Gmail, search

08/05/2014 13:57 (Tech and Gadgets - MSN CA)

Hackers confused Iranian scientist by blaring AC/DC in nuke lab

08/07/2014 07:36 (Crowdfunding Today)

...a massive conference room at the Mandalay Bay Wednesday, legendary **computer security** visionary Mikko Hypponen had a funny story to tell. The...

US DHS contractor gets hacked

08/07/2014 06:17 (Help Net Security)

"Our internal IT security team recently identified an apparent external **cyber**-**attack** on USIS corporate network. We immediately informed federal...

Deploying and monitoring honeypots made easy

08/07/2014 03:43 (Help Net Security)

...the system, observed successful attacks, and attempted/successful **malware** activity on the host. This automated and integrated approach to honeypots...

Data breach news hits during security conference

08/06/2014 17:37 (Federal Times)

...coincidentally, some say was also the opening of Black Hat, a popular **computer security** conference held in Las Vegas each August. It is followed by DefCon,

TSA Checkpoint Systems Found Exposed on the Net

08/06/2014 15:00 (Dark Reading)

...or expertise to understand it," he says. In addition, **hacking** one of these devices is fairly simple, especially when the devices contain **backdoor**,

Cybersecurity: Why It's a Team Sport

08/08/2014 09:25 (GovInfoSecurity)

...Group, which was responsible for some of NSA's advancements in **cyber defense**. Follow Eric Chabrow on Twitter: @GovInfoSecurity By Eric Chabrow,

Smart grid attack scenarios (understand the threat to defend against it)

08/08/2014 08:23 (Smart Grid News)

...of Everything hub. Jesse Berst is How to keep your smart meters safe from **attack** (and not just **cyber**-attacks) Smart meters are a "time bomb"

Russia-linked cyber attack on Ukraine PM's office

08/08/2014 07:48 (CNBC)

Russia-linked **cyber attack** on Ukraine PM s office Dozens of computers in the Ukrainian prime minister's office and at least 10 of Ukraine's embassies...

Nissan investigates claims its Infiniti car is 'most hackable'

08/08/2014 06:50 (ComputerWorldUK.com)

...protect against cyber-attacks. Bart Jacobs, professor of **Computer Security** at Radboud University Nijmegen in the Netherlands, recently expressed...

The Internet of Things Brings Far-Reaching Security Threats

08/08/2014 05:48 (Network World)

...a more hands-on CIO and an organizational rethinking. WASHINGTON **Security** pros routinely cite poor **cyber** hygiene as one of their top concerns.

How hackers used Google in stealing corporate data

08/08/2014 03:46 (ComputerWorldUK.com)

...disclose the name of the victims. The unidentified **hackers** had used **spear**-**phishing** attacks to compromise the systems and then used the malware...

Former top brass say cyberspace key in new Japan defense rules

08/07/2014 17:28 (Stars and Stripes)

...more than five times the current numbers. By comparison, Japan s **Cyber Defense** Unit, launched in March to detect and respond to attacks on the...

Jack Huffard, Tenable Co-Founder, on Changing the 'Hacker' Discourse and Staying Abreast of Disruptive Cyber Trends

08/07/2014 16:43 (WashingtonExec)

...providing it. What do you think will be most disruptive to the **cyber security** market during the next five years? Jack Huffard: The thing that...

FBI hosts ‘CyberCamp’ for high school students

08/07/2014 15:53 (Charlotte Observer)

...of those type of skills in the U.S., Gardner said. Growth in **cyber**-**forensics** is expected to grow from 13 to 22 percent in the next five years,

Playing Russian Roulette with Internet Security

08/07/2014 15:46 (SecurityInfoWatch.com)

...even personal websites. Sami Nassar, who currently leads the **digital security** products for the **cyber security** markets at NXP Semiconductors,

Attack Harbors Malware In Images

08/07/2014 15:45 (Dark Reading)

...the intelligence community and most recently terror groups, but a **cyber crime** gang has been spotted using the stealth technique of embedding...

Smart Nest thermostat easily turned into spying device

08/11/2014 08:55 (Help Net Security)

...that the OS level security checks that should prevent the installation of **malware** on the device can be easily bypassed. Amazingly enough, it...

Turns Out Your Complex Passwords Aren’t That Much Safer

08/11/2014 06:38 (Wired)

Turns Out Your Complex Passwords Aren t That Much Safer When the **computer security** company Hold **Security** reported that more than 1.2 billion...

The New Healthcare Vulnerability: Closing the Cybersecurity Leadership Gap

08/11/2014 06:17 (Fort Mill Times)

...Gartner. "Many traditional security officers will change their titles to **digital** risk and **security** officers, but without material change in their scope,

Animal hackers: War Kitteh and Denial of Service Dog sniff out insecure Wi-fi

08/11/2014 04:24 (The Guardian)

...convention in Las Vegas showcased a pair of projects mixing pets with **computer security**. War Kitteh and Denial of Service Dog were both the work...

The art and science of detecting emerging threats

08/11/2014 04:06 (Help Net Security)

...mathematicians at the University of Cambridge, and applied to the **cyber security** challenge to deliver the first Enterprise Immune System. The...

Irish Bookie Follows Stolen Client Cache to Ontario Basement

08/11/2014 02:45 (Washington Post - Bloomberg)

discount retailer. Bumble B For Paddy Power, the story began with a **cyber attack** in late 2010, according to a company statement on July 31 and...

Snowden leaks prompt firms to focus cyber security on insider threats

08/10/2014 16:54 (Los Angeles Times)

Snowden leaks prompt firms to focus **cyber security** on insider threats At this week s Def Con hacker gathering in Las Vegas, Tess Schrodinger...

Security experts call for government action against cyber threats

08/09/2014 19:33 (Yahoo! News)

...enemies using malware to sabotage utilities, wipe out data stored on **computer** drives, and steal **defense** and trade secrets. Such fears and proposals...

At 'Cyber Challenge,' The Best Hacker Wins

08/08/2014 19:24 (CBS Chicago)

...Hacker Wins Sign Up (CBS) This week, the biggest-ever **cyber attack** targeting more than 400,000 websites became the latest reminder of how Sign...

Data breaches and high-risk vulnerabilities continue to dominate

08/12/2014 09:16 (Help Net Security)

...of mobile ransomware and two-factor authentication-breaking **malware** has emerged in response to technological developments in the online banking...

Why utilities need to worry about the 10 most vulnerable consumer devices

08/12/2014 08:31 (Smart Grid News)

...smart meter (Utilities: better find out before the criminals do) How to keep your smart meters safe from **attack** (and not just **cyber**-attacks)

Increase in Hacking Cases Brings Urgency to Cybersecurity, Says WVU Expert

08/12/2014 07:14 (Technology News)

changing account names or user names (if possible), updated **computer** anti-**virus** software and multistep verification will also reduce vulnerability.

Let us help you defend cars from cyber-attacks: Hacking group to 'Automotive CEOs'

08/12/2014 07:12 (Tech Times)

...provide assistance to automotive companies looking to improve their cars' **security** against **cyber**-attacks. This program includes required testing of...

How To Fix Hopelessly Hackable Power Plants? Start With Beer

08/12/2014 07:07 (Forbes.com)

...s the key to exposing a dirty secret amongst manufacturers of **critical infrastructure** technology, one the **hacker** world has known for some time:

RECRUITING HACKERS

08/12/2014 06:25 (Yahoo! News)

...secure U.S. defense contractors are turning to hackers for help in their **war** on **cyber** criminals. Some of the most secure U.S. defense contractors...

How hi-tech cars without keys have put thieves back in the driving seat

08/12/2014 04:46 (PressDisplay.com)

Hackers learn some new tricks at Def Con on avoiding surveillance

08/11/2014 20:37 (Tech Times)

...year's conference, Philip Polstra, associate professor of **digital forensics** at Bloomsburg University of Pennsylvania, discussed low-tech solutions...

Two new Gameover Zeus variants in the wild

08/11/2014 16:27 (SC Magazine)

...closely on the Gameover Zeus code, which was being delivered through **phishing** emails claiming to be from legitimate banks. That variant also used...

Android backdoor lurking inside legitimate apps

08/13/2014 04:33 (Help Net Security)

...applications from dubious sources and to stick to the official Google Play store. **Malware** does show up from time to time there, but it is much better...

Magnitude exploit kit changes tack to make money from CryptoWall ransomware

08/13/2014 03:38 (Computerworld Malaysia)

...Blackhole demise signal end of exploit kit era? The Russian Magnitude **malware** exploit kit has moved on to the territory vacated by the defunct...

Malware is less concerned about virtual machines

08/12/2014 19:55 (ComputerWorld)

Malware is less concerned about virtual machines Symantec finds most **malware** doesn't quit if it runs on VM, which used to be a sign it was being...

Standardizing complaints, sharing cyber info and tracking Ebola

08/12/2014 17:14 (Federal Computer Week)

...communication. One participant was quoted in the report on DHS' **Enhanced Cybersecurity Services** program as saying that "the threat indicators provided were...

Silicon Valley is becoming bigger player in Washington

08/12/2014 16:53 (Centre Daily Times)

...priorities, Wright said: Immigration reform, corporate tax reform, **cyber security** and net neutrality. Government surveillance, as revealed by the...

Cyber Uncertainty [National Guard]

08/12/2014 15:04 (Technology News)

Cyber Uncertainty [National Guard] (National Guard Via Acquire Media NewsEdge) Governors want to tap the Guard's growing **cyber** capability. (National...

Cyber Infiltration During Operation Protective Edge

08/12/2014 15:00 (Forbes.com)

...terror organizations independent cyber units. To operate a successful **cyber attack** requires determination of targets, timing of the **attack** and...

NIST ICS, SCADA, Test Bed

08/12/2014 14:17 (Isssource.com)

...create a test bed to examine industrial control systems for **cyber security** The National Institute of Standards and Technology wants to create...

A timely warning from the feds: Bitcoins are the 'Wild West'

08/12/2014 10:33 (Los Angeles Times)

...that bitcoins are secure, they are vulnerable to hacks, thefts of **digital security** keys, and scams. Bogus exchanges and traders lie in wait to...

Who Receives Hacker Threat Info From DHS?

08/11/2014 17:32 (Nextgov)

...16 so-called critical infrastructure industries. The **Enhanced Cybersecurity Services** program feeds confidential alerts about the digital hallmarks,

WikiLeaks' Assange hopes to exit London embassy if UK lets him
http://www.reuters.com/article/2014/08/18/us-wikileaks-assange-idUSKBN0GI0QP20140818

Hackers hit US supermarket giant SuperValu in latest cyber crime attack
http://www.thedrum.com/news/2014/08/17/hackers-hit-us-supermarket-giant-supervalu-latest-cyber-crime-attack-0

Cyber forensics: taking tips from a detective's playbook
http://www.gsnmagazine.com/node/42202?c=cyber_security

Ebola fear used as bait, leads to malware infection
http://www.deccanchronicle.com/140818/technology-science-and-trends/article/ebola-fear-used-bait-leads-malware-infection

NSA works to automatically detect attacks, return strikes from foreign adversaries
http://www.scmagazine.com/nsa-works-to-automatically-detect-attacks-return-strikes-from-foreign-adversaries/article/366382/

Meet the Man Leading the Snowden Damage Investigation
http://www.defenseone.com/threats/2014/08/meet-man-leading-snowden-damage-investigation/91631/

U.S. Intelligence Can't Stop the Next Snowden for Years
http://www.thedailybeast.com/articles/2014/08/18/spy-games-us-intelligence-agencies-overdue-for-new-protocols-to-detect-leakers.html

10 hot programming languages that are on the rise
http://www.computerworld.com/slideshow/detail/149179/

Gyroscopes on Android devices can be used to eavesdrop on users' conversations
http://www.net-security.org/secworld.php?id=17266

Chinese man indicted over theft of Boeing C-17 secrets
http://www.computerworld.com/s/article/9250448

Premier FBI cybersquad in Pittsburgh to add agents
http://www.stripes.com/news/us/premier-fbi-cybersquad-in-pittsburgh-to-add-agents-1.298698

Security Expert Discovers Hole In Satellite Communications
http://www.nbcchicago.com/investigations/Security-Expert-Discovers-Hole-In-Satellite-Communications-271779971.html

How to Save the Net: Break Up the NSA
http://www.wired.com/2014/08/save-the-net-bruce-schneier/

How to Save the Net: A CDC for Cybercrime
http://www.wired.com/2014/08/save-the-net-peter-singer/

Why global efforts to combat cybercrime are so difficult
http://techpageone.dell.com/uncategorized/why-global-efforts-to-combat-cybercrime-are-so-difficult/#.U_NhA2PfX1U

US: Cybercom Expands Capacity In Defense Of Networks, Nation
http://www.eurasiareview.com/19082014-us-cybercom-expands-capacity-defense-networks-nation/

Michael Rogers: Cybercom Must Be Flexible to Face Cyber Challenges
http://www.executivegov.com/2014/08/michael-rogers-cybercom-must-be-flexible-to-face-cyber-challenges

Bugat Malware Adds GameOver Functionality
http://www.infosecurity-magazine.com/news/bugat-malware-adds-gameover/

Pro-Syrian Malware Increasing in Number, Complexity
http://threatpost.com/pro-syrian-malware-increasing-in-number-complexity

Hackers take control of Internet appliances
http://www.wcnc.com/story/technology/2014/08/19/hackers-take-control-of-internet-appliances/14274317/

Obama Admin. Says Hackers Could Steal Personal Info if They Share Security Practices for Healthcare.Gov
http://www.theblaze.com/stories/2014/08/19/obama-admin-says-hackers-could-steal-personal-info-if-they-share-security-practices-for-healthcare-gov/

Scientists, Not Politicians, Should Regulate NSA Surveillance
http://motherboard.vice.com/read/we-should-ask-scientists-what-they-think-about-nsa-surveillance

Government's Response To Snowden? Strip 100,000 Potential Whistleblowers Of Their Security Clearances

'Chinese crims' snatch 4.5 MILLION patient files from US hospitals
http://www.theregister.co.uk/2014/08/18/hospital_chain_claims_chinese_hackers_stole_45_million_user_details/

Digital data links Inland Empire men to suspected terrorist activity
http://www.sbsun.com/general-news/20140819/digital-data-links-inland-empire-men-to-suspected-terrorist-activity

Cyber Crime Opens New Portals Offers New Solutions

http://guardianlv.com/2014/08/cyber-crime-opens-new-portals-offers-new-solutions/

Kicking the stool out from under the cybercrime economy
http://www.csoonline.com/article/2466506/data-protection/kicking-the-stool-out-from-under-the-cybercrime-economy.html

Syrian malware is lurking, is dangerous
http://www.deccanchronicle.com/140820/technology-latest/article/syrian-malware-lurking-dangerous

Malware married to software in undetectable attack
http://www.theregister.co.uk/2014/08/20/malware_married_to_software_in_undetectable_attack/

Hacking Traffic Lights Is Apparently Really Easy
http://time.com/3146147/hacking-traffic-lights-is-apparently-really-easy/

Smart city control networks being architected more securely than SCADA
http://www.cso.com.au/article/552839/smart_city_control_networks_being_architected_more_securely_than_scada/

Mobile device security: Tackling the risks
http://www.net-security.org/article.php?id=2101

'Reveton' ransomware adds powerful password stealer
http://www.computerworld.com/s/article/9250503

How to Save the Net: Keep It Open
http://www.wired.com/2014/08/save-the-net-vinton-cerf/

Summer program at NYU Poly teaches cybersecurity to young women
http://technical.ly/brooklyn/2014/08/20/summer-program-nyu-poly-teaches-cybersecurity-young-women/

The UPS Store says malware found on systems of 51 stores
http://www.pcworld.com/article/2538380/the-ups-store-says-malware-found-on-systems-of-51-stores.html

A New Attack Secretly Binds Malware to Legitimate Software Downloads
http://gizmodo.com/a-new-attack-secretly-binds-malware-to-legitimate-softw-1624894033

How Hackers Could Mess With 911 Systems and Put You at Risk
http://www.wired.com/2014/08/how-hackers-could-mess-with-911/

Google Says HTTPS Is A Ranking Signal, But It's Not Really
http://searchengineland.com/google-says-https-ranking-signal-really-201058

Collective self-defence: What Japan's new defence policy means for international cooperation on cyber security
http://www.eastasiaforum.org/2014/08/21/collective-self-defence-what-japans-new-defence-policy-means-for-international-cooperation-on-cyber-security/

'Tech support' scammers using fake downloads to snare new victims
http://www.theguardian.com/technology/2014/aug/21/tech-support-scammers-fake-downloads-new-victims

Report: Devastating Heartbleed Flaw Was Used in Hospital Hack
http://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/

DARPA Uses Preteen Gamers to Beta Test Tomorrow's Military Software
http://motherboard.vice.com/read/darpa-uses-preteen-gamers-to-beta-test-tomorrows-military-software

Targeted spear phishing campaign targets governments, law enforcement
http://www.scmagazineuk.com/targeted-spear-phishing-campaign-targets-governments-law-enforcement/article/367133/

White House cybersecurity czar brags about his lack of technical expertise

http://www.vox.com/2014/8/21/6053819/white-house-cybersecurity-czar-brags-about-his-lack-of-technical

Experts discover history of malware infections on network of Community Health Systems
http://www.scmagazine.com/experts-discover-history-of-malware-infections-on-network-of-community-health-systems/article/367454/

China's Cyber Warriors Keep Clicking at Taiwan Shows Reality of Detente
http://www.bloomberg.com/news/2014-08-21/china-s-cyber-warriors-keep-clicking-at-taiwan.html

Agencies Get New Guidelines for OK'ing Apps
http://www.nextgov.com/mobile/2014/08/new-agency-guidelines-apps/92108/?oref=ng-dropdown

NATO needs strong policy against cyber threats
http://www.bostonglobe.com/opinion/2014/08/22/nato-needs-strong-policy-against-cyber-threats/cetoHkprGGZHMUAjfOhjHJ/story.html

NSA official: 'Much easier' to explain operations after Snowden

http://thehill.com/policy/technology/215694-nsa-official-much-easier-to-explain-operations-after-snowden

How to Save the Net: Build a Backup
http://www.wired.com/2014/08/save-the-net-danny-hillis/

Critical Delphi and C++Builder VCL library bug found
http://www.net-security.org/secworld.php?id=17280

Extracting encryption keys by measuring computers' electric potential
http://www.net-security.org/secworld.php?id=17282

US agencies to release cyberthreat info faster to healthcare industry
http://www.computerworld.com/s/article/9250579

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

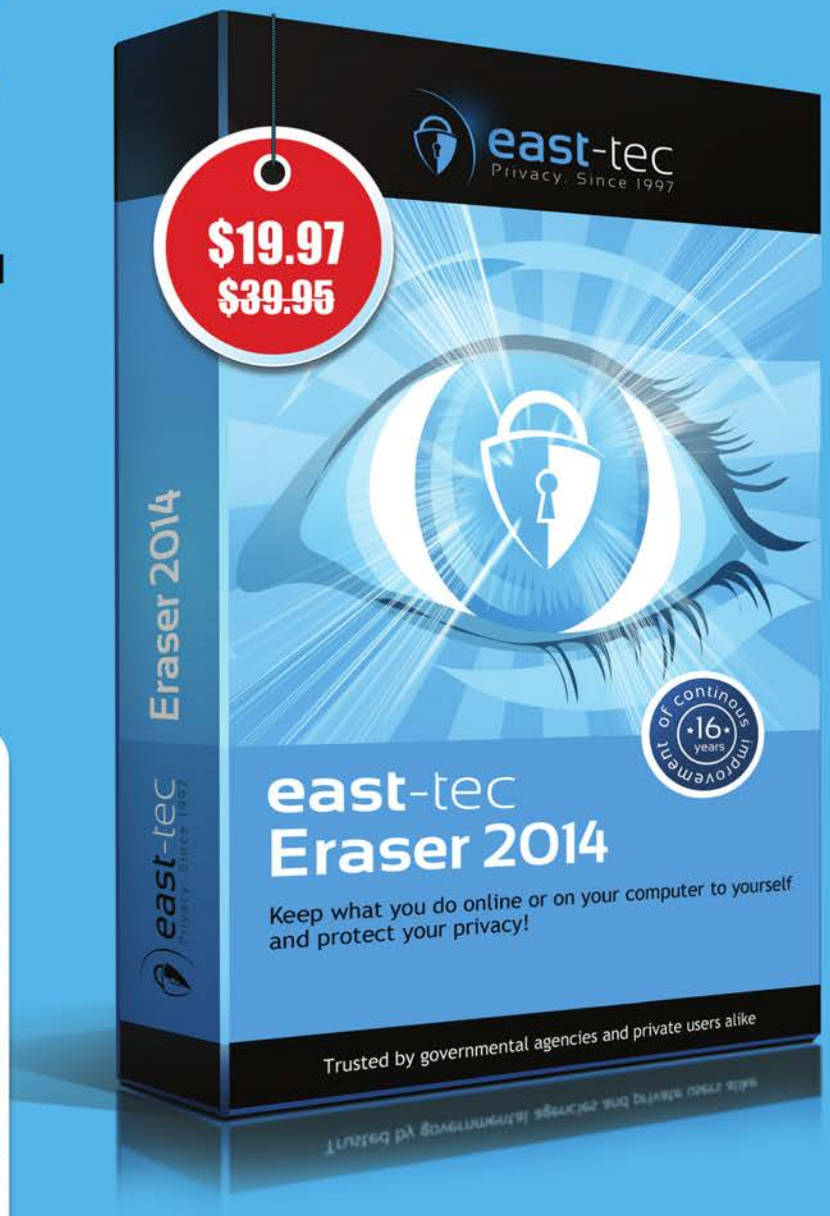
Cyber Defense Magazine - Cyber Warnings rev. date: 08/25/2014

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

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



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014

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