CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Machine Learning
SMB Cybersecurity
Healthcare Security
Phishing Defense

May 2016

MORE INSIDE!

CONTENTS

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Michael Sabo
Slavik Markovich
Jeff Hussey
Dylan Sachs
Rene Paap
Carl Wright
Aviv Grafi
Thorsten Held
Gary S. Miliefsky
Amrita Mitra
Heather Lee
Don Jackson
Milica Djekic
Sarah Brown
Dilip Pillaipakkamnatt

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®

Phishing Attacks and Ransomware Getting Smarter This Year

Friends,

Remember the days when you received a poorly written email with misspelled words and bad grammar from an email address you never had in your contact list? You quickly knew something was 'phishy' and simply ignored it. Well, my friends, those days are long gone. As this year kicked off with a bang of attacks against Small to Medium Sized Enterprises (SMEs), especially in Health care, we keep hearing story after story of some organization paying the Ransomware fees. Now, in the UAE, there were $3M in payments this month by banks to decrypt their systems – yes, they paid that much to 'unwind' the malware and ensure their files were not lost forever. But why should anyone pay these cyber criminals? It's really simple. Most organizations are not prepared, especially the SMEs, for the flood of Ransomware making it onto their networks. This is becoming a very lucrative business and with the advent of anonymous currency, the 'bitcoin', it's easy to get paid and disappear (or come back later to the same victim for more extortion). Yes, if you press for it, you can track down these hackers but it's usually too late and you've lost the data. Oh, the precious data! How can we risk losing it, ever? Just pay the ransom, right? Wrong!

The real reason we're seeing so much successful cyber crime extortion is simple – it's more than employee training – it's about doing FREQUENT (even CONTINUOUS) backups and testing them. You could avoid paying ransomware fees if you simply wipe the drive, re-image, then restore. What? You forgot to test your backup system? You've never tested a restore process? Aha, now we have it – the real issue is better PROACTIVE information security. To top that off, we need to rapidly (and I mean in seconds or less), isolate the infected system and take proactive measures to resolve the issue. I have seen very few companies in the market today that focus on BREACH PREVENTION but that's where the future of INFOSEC should be going. It's about real-time encryption, backups, testing restore processes, nailing your re-imaging process and ensuring instant ability to quarantine systems with users who fall prey to phishing attacks, remote access Trojans and ultimately the latest and most successful threat – Ransomware.Training and retraining employees is very important but human frailty and error always lead to intranet breaches and infections.

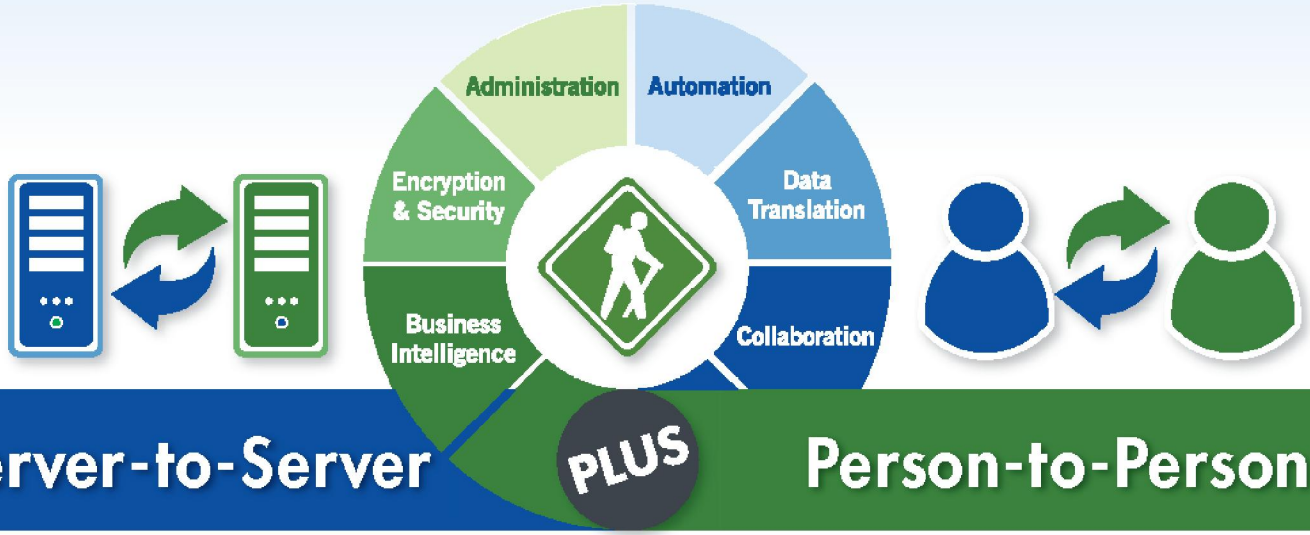
With that said, I hope you find some additional new ideas that will help you not be the next victim, in this May 2016 edition of Cyber Warnings.

To our faithful readers, Enjoy

Pierluigi Paganini

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

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

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

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

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

Visit GoAnywhere.com for a FREE trial.

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

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

One of the Largest North American Railroads

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

GoAnywhere.com 800.949.4696

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

Applying Machine Learning and Behavioral Analysis to Address the Cybersecurity Skills Shortage

It's no secret there's a severe skills shortage in cybersecurity. More than 209,000 cybersecurity jobs in the U.S. alone are presently unfilled according to a 2015 Peninsula Press analysis of data from the Bureau of Labor Statistics. In addition, according to Peninsula Press job openings are up 74 percent over the past five years.

The skills shortage situation is expected to deteriorate even further over the next several years, and the situation is stressing security staffs in organizations of all sizes.

As an example, consider the massive security breach at Target, where more than 40 million credit card numbers were stolen. It was widely reported that Target missed alarms that clearly indicated a breach was in progress.

However it's important to realize that Target, like many other organizations, is under constant attack. Target receives many thousands of attacks everyday and therefore alarms are continuous. There simply aren't enough security personnel to chase down each alarm and remediate it.

When we look across the IT security landscape it's just not possible to build the talent pool rapidly enough to fully address this critical skills shortage of individuals needed to combat constantly evolving threats – automation is the answer.

The old adage "work smarter, not harder" is certainly applicable in this case. First and foremost the security industry needs to move beyond labor intense security mechanisms that are at the same time are continually becoming less and less effective.

Traditional early generation security technologies such as signature files, white lists, and black lists are very labor intense. These technologies were once the bedrock of cybersecurity in the later part of the last century.

However, because of the rapidly evolving threats this approach now consumes a large amount of staffs' time writing and testing rules.

This is occurring even though signature files, white lists, and black lists are ineffective against modern cyber attacks such as the Advanced Persistent Threat (APT).

The legacy approaches are also notoriously poor at identifying attacks in real-time and also generate large numbers of false positive alarms. Rules and signatures are often written too broadly and flag not only illegitimate traffic but also legitimate traffic - resulting in a false positive alert.

Having security staff chase down false positives throughout the day is highly unproductive and further exasperates the skill shortage. But old habits die hard.

Machine learning and behavioral analysis security technologies are now being applied to endpoint security, web application security, intrusion detection, and database security.

DB Networks DBN-6300 is an example of machine learning and behavioral analysis technology applied to the database tier.

Machine learning in combination with behavioral analysis is able to immediately identify database attacks and compromised credentials without the use any predefined rules or signature files whatsoever.

Field experience has proven these technologies to be highly effective, without generating false positives, and, importantly, requiring minimal operation support.

As deployments of machine learning and behavioral analysis-based IT security occur across the IT infrastructure, these smart security systems will eventually be integrated into a unified architecture providing full-spectrum autonomous cybersecurity.

At that point the information security skills shortage will be essentially solved. Information security personnel will finally be to apply their skills to architecting secure systems rather than chasing false alerts and devising signature files based on the last week's threat intelligence.

About the Author

Michael Sabo, VP Marketing for DB Networks:
Michael leads the market research, positioning, communications, and promotions for DB Networks. Michael's extensive background in marketing, strategic planning, and product engineering was gained from his tenure at Intel Corporation, US West (now CenturyLink), and Contel (now Verizon) as well as start-ups AirFiber and Rhythms NetConnections.

In 1995 while at US West, he developed and launched !NTERACT Internet Security as an earliest example of a cloud-based Managed Security Service Providers (MSSP) service.

Michael earned a B.S. in Computer Science from Wright State University and Masters degree from the University of Denver.

Nice Global Forum

International Congress on Homeland Security and Crisis Management

25-28 October 2016 | Nice, France

Programme

- Major risks (environmental, climatic, seismic, industrial, CBRN) / Risques majeurs (environnementaux, climatiques, sismiques, industriels, NRBC)
- Crisis management / Gestion de crises
- Civil defence and emergencies / Sécurité civile
- Urban security / Sécurité urbaine
- Counter-terrorism / Contre-terrorisme
- Economic intelligence / Intelligence économique
- Cybercriminality / Cybercriminalité
- Communication, social media / Communication, réseaux sociaux
- Safe and Smart City
- Corruption & Security / Corruption & Sécurité

Forum - Congress - Exhibition / Forum - Congrès- Exposition

- 4 chairmen: Boaz Ganor, Brian Jenkins, Alain Bauer, Jean-Louis Bruguière
- 1 International Forum with over 60 international mayors and governmental bodies / 1 Forum avec plus de 60 maires internationaux et des partenaires gouvernementaux
- 60 international delegations / 60 délégations internationales
- 45 international expert speakers / 45 intervenants experts internationaux
- 40 security industrial leaders / 40 industriels du domaine de la sécurité
- Heads of global security services / Des directeurs de sécurité des entreprises
- Heads of law enforcement agencies / Des chefs des forces de l'ordre gouvernementales

www.niceglobalforum.org

Paragon Group

Congress Secretariat: Paragon Group
www.paragong.com | Tel: +41 22 5330 948
18 Avenue Louis-Casai | 1209 Geneva | Switzerland
Email: secretariat@niceglobalforum.org
www.niceglobalforum.org

NICE CÔTE D'AZUR Tourisme et Congrès

MÉTROPOLE NICE CÔTE D'AZUR

Is Your SOC Staffed Appropriately?

By Slavik Markovich, co –founder and CEO of Demisto
www.demisto.com

When starting to build a Security Operations Center (SOC), your first consideration should be your team. Staffing a SOC can be more difficult than expected. How many people will you need to employ? What training do they require? How should the team be structured? How do you plan for capacity?

These and other questions must be clearly answered in order to provide an educated approach to SOC resource planning. Guessing and winging it as you go along is just not an option. Before investing time, effort and resources, make sure that your SOC team is staffed appropriately.

Structure Your SOC Team

The standard structure of an SOC team includes Alert Analysts, Incident Responders, Subject Matter Experts and SOC Managers, all of whom should all be experienced IT and networking professionals trained in computer science, cryptography or network engineering.

Analysts should be the first to be hired, since they support the initial build-out of the SOC, as explained below.

The SOC team structure is integrally related to the level of expertise an organization has in-house. You may already have employees that are able to fulfill some or all of the roles, or you might need to consider outsourcing (via managed security service providers) or contracting specialists to provide surge incident response (IR) support. Many companies adopt a solution that is a combination of these options.

Below is a summary of the functions of each member of the SOC team and the skill sets they should possess:

Alert Analyst:

- Constantly monitors the alert queue
- Prioritizes security alerts
- Checks on the operational efficiency of security sensors and endpoints
- Compiles data and background material needed by the Incident Responders to perform their job

The Alert Analyst should be trained in intrusion detection; alert triage processes; security information and event management (SIEM); host-based investigative training; and other tool-specific training.

Alert analysts should be given playbooks and procedures to decide on the priority and assignment of alerts.

Incident Responder:

- Performs deep incident analysis by correlating data received from the Alert Analyst and other sources
- Identifies if a critical system or data set has been impacted and recommends solutions
- Collects and correlates threat intelligence related to the incident and uses the data to investigate
- Assists in decision making using different types of software, e.g. phishing, malware and ransomware.

The Incident Responder should be trained in advanced network forensics, host-based forensics, incident response procedures, malware assessment, network forensics, log reviews and threat intelligence.

Subject Matter Expert:

- Proactively searches for breaches in order to avoid escalated incidents
- Conducts deeper analysis on complex incidents including malware reversing, log analytics, forensics and response planning
- Contributes to developing, tuning and implementing threat detection analytics

The Subject Matter Expert possesses in-depth knowledge of network, endpoint, threat detection, forensics, malware reverse engineering, data aggregation and the functioning of specific applications or underlying IT infrastructure.

SOC Manager:

- Directs the SOC and provides input to the company's larger security strategy, serving as organizational point person for business-critical incidents
- Prioritizes tasks in order to detect, investigate and mitigate incidents that could impact the business
- Creates a workflow model and ensures that reporting and documentation are maintained accordingly
- Implements standardized operating procedures (SOPs) for handling incidents to guide analysts through the triage and response processes
- Manages resources, personnel, budget and scheduling to meet SLAs

Besides possessing excellent people management skills, the SOC Manager should be trained in Project Management and Incident Response Management. Certifications could include CISSP, CISA, CISM or CGEIT.

Plan for Capacity

SOCs are typically staffed eight hours a day, five days a week or around the clock. All shifts should include at least two analysts with clearly defined responsibilities. A standard 24/7 SOC should ideally be maintained by at least seven staff members; otherwise, procedures should be implemented for off-hours monitoring, providing a one-hour overlap for shift transfer and a floater to cover holidays, sick leave and time off when needed.

Planning for capacity in each group is a function of workload and types of incidents flowing. It is critical to predict the SOC's workload, in order to be able to identify the skillsets required to effectively manage all incoming threats, attacks and incidents. Furthermore, the types of incidents faced by the SOC, e.g. phishing, malware, data leakage, cyber-attacks, will determine the level of complexity involved.

A proven method for capacity planning in an SOC team is calculating and quantifying the number of incidents occurring through the network per day, in order to gain an understanding of the incident flow. Based on the incident flow, resources can be effectively allocated, from assessing an alert, to escalation, and through to resolution.

As you begin building a new SOC, staffing your team appropriately will lead to a smooth startup and build-out over time. This, in turn, should ensure a quick return on investment.

About the Author

Slavik Markovich is co-founder and CEO of Demisto. Prior to co-founding Demisto, he was VP & CTO of database technologies at McAfee (Intel Security). He got to McAfee via the acquisition of Sentrigo, a database security startup, where he was co-founder and CTO. Slavik has over 20 years of experience in infrastructure, security and software development. Previously, Slavik was vice president of R&D and chief architect at DB@net, a leading IT architecture consultancy firm.

Slavik is a renowned authority on Oracle and Java/JavaEE technologies, and has contributed to open-source projects such as Spring Framework Toplink integration (later incorporated by Oracle). He is a regular speaker at industry conferences. He holds a BS degree in Computer Science.

GREMLIN NETWORKS

The Much Needed Evolution of IP

Jeff Hussey, CEO, Tempered Networks

When was the last time you saw someone cruising to work in a Gremlin? Unless it was a movie character, we're guessing it wasn't very recently. The AMC Gremlin, which launched in 1970, has achieved cult-like status among car collectors, but you're not likely to see one on the roads today. What if I told you that the language powering most of our Internet communications today is the technology equivalent of the Gremlin? Because that's what it really is.

Four Score and Seven Years Ago

The protocol we're using today to power global commerce over the Internet was developed almost 50 years ago. Development efforts in the late 1960s and early 1970s created the TCP/IP protocol, which was originally designed to allow smaller local networks communicate between short distances in ways they had never before. However, at the time of its inception, reliability was the only concern as the idea of security was a man with a machine gun guarding the facility. Despite being an incredible development, we are left with a protocol that is incredibly reliable, yet inherently unsecure as trusted identities were not part of the design. This has led to today's environment, where components are bolted on for security, rather than baked in from the start. And, given the number of data breaches we see in the headlines, we can all see how that's working out.

Cyber Kill Chain

Federal agencies have to find new solutions to the problems our existing security solutions can't handle. Current solutions involve huge amounts of operational complexity and require an ever-increasing number of IT staff to maintain. In many military environments (and even in many civilian ones), staff with the specialized expertise is tough to come by. To combat the increasing amount of security threats, a new approach to securing critical infrastructure and assets is needed, which targets attackers' processes and can quickly scale to greater levels while being managed by non-IT personnel.

Understanding the phases of a cyber attack helps clarify why a new security protocol is necessary. The "kill chain" model is one that's familiar to most readers, and one that can be applied to cyber threats as one of the advanced persistent threats (APTs) defense personnel must manage:

Today's hackers, like any other adversaries, begin their attacks with the recon phase. That's often the most efficient and effective place to stop an attack. Assets protected by our solution

are cloaked and invisible from the underlying network. By hiding critical infrastructure, the attack is stopped at the very first phase—recon—as attackers can't see or identify which assets are on the network or what data they may contain. The attack stops before it has a chance to begin.

The Much Needed Evolution of IP

The time has more than come to re-evaluate the Gremlin of Internet protocols, TCP/IP. The Internet Engineering Task Force recently approved a standard-track network security protocol: The Host Identity Protocol, which many in the IETF community recognize as the next big change in IP-architecture. The protocol has been under development for nearly 20 years, in coordination with standards bodies, as well as many large corporations (Verizon, Ericson, Yokogawa, etc.).

HIP is an alternative encryption technology that was first deployed within the defense and aerospace industry, where nation-state attacks occur every hour. Specifically designed to be secure by default, HIP shifts the network trust model completely by introducing trusted cryptographic identities within any network. It's like the Gremlin riding around inside an armored truck.

Not only does our solution help stop attacks before they begin, it removes another key enemy of security—complexity. Through the simplicity of our centralized orchestration engine, the number of IT administrators needed to maintain security is significantly reduced. An IT department can maintain centralized governance of security, while assigning controls and access to designated operations teams without compromising the safety of the network. Field personnel with basic IT skills can now maintain and operate secure networks with limited technical support, and a smaller number of skilled IT personnel can manage critical infrastructure security.

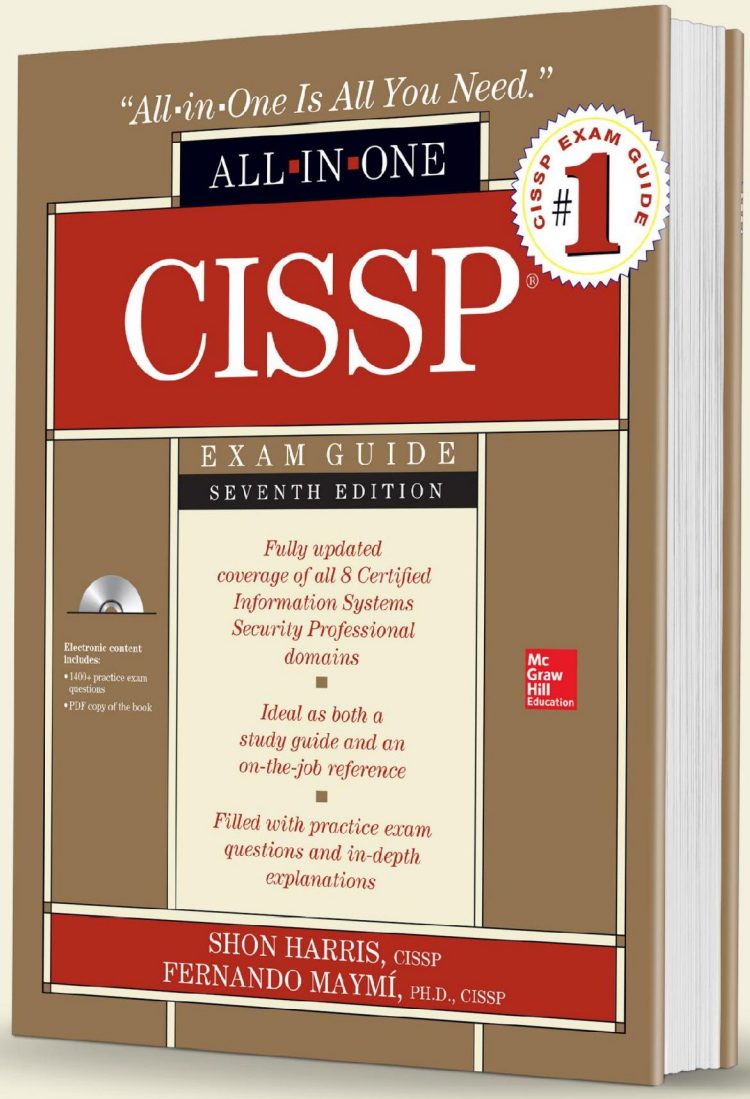
The threat landscape for any organization has radically changed within the last decade. To meet these new challenges, we need to step away from the traditional solutions that have been protecting networks for a long time, and into the 21st century. Rather than pouring thousands of dollars and staff hours into trying to maintain a secure perimeter, moving to a new approach makes security both stronger and more scalable. When cloaking becomes the new perimeter, both operations and field teams can manage security easily and stop cyber attacks before they have the chance to begin.

About the Author

Jeff Hussey has been the President and CEO of Tempered Networks since August 2014. Hussey, the founder of F5 Networks, is an accomplished entrepreneur with a proven track record in the networking and security markets. He maintains several board positions across a variety of technology, non-profit and philanthropic organizations and currently is the chairman of the board for Carena and chairman and co-owner of Ecofiltro and PuraVidaCreateGood.

The #1 CISSP® training resource—fully revised for the new exam domains

SAVE 30%!



Thoroughly updated for the latest release of the Certified Information Systems Security Professional exam, this comprehensive resource covers all exam domains, as well as the new 2015 CISSP Common Body of Knowledge developed by the International Information Systems Security Certification Consortium (ISC)²®. Written by leading experts in IT security certification and training, this completely up-to-date self-study system helps you pass the exam with ease and also serves as an essential on-the-job reference.

Electronic content: 1400+ practice questions, including new hot spot and drag-and-drop questions.

"Essential for those pursuing CISSP certification, and should be part of every cybersecurity professional's library."

–From the Foreword by Rhett Hernandez, Lieutenant General, US Army Retired; Former Commander, US Army Cyber Command; Current West Point Cyber Chair, Army Cyber Institute

CISSP All-in-One Exam Guide, Seventh Edition
Shon Harris and Fernando Maymí
ISBN: 0-07-184927-0
List Price: $80.00 **Your Price:** $56.00

SAVE 30% at www.mhprofessional.com
with promo code CISSP0516

@MHComputing

Available in print and as an eBook

Mc Graw Hill Education

Why MX Records Matter in the Fight Against BEC and Spear Phishing

By Dylan Sachs, BrandProtect

In March 2016, the HR department of a regional financial institution received emails from their CEO requesting copies of sensitive employment files, including employee personal information, such as full names, mailing addresses, phone numbers, SSNs, and other highly-sensitive PII. Because of the sensitive nature of the information in the files, the alert HR team double-checked with their CEO before they complied with the request.

It was a good thing they did. The email was not from their CEO.

It was a socially engineered spear phishing or BEC attack, originating from a domain that was similar enough to the institution's regular domain that it could have easily been mistaken for a legitimate email.

Having sidestepped a bullet, the institution sought expert help to better understand what had happened. They turned to BrandProtect, whose Incident Response team quickly determined that that the rogue domain used to send and receive the attacking emails, had been registered only the day before the attack, and a quick MX check of the newly registered domain confirmed that the mail server listed in the MX record of the domain matched that found in the header details of the suspicious email.

Within one hour, the BrandProtect team, working with the appropriate registrar and server host, had the rogue domain taken down. With the domain suspended, and the server taken down, the perpetrators were no longer able to use this infrastructure to target the company's employees.

This BEC attack sought sensitive information, but other BEC attacks like this one carry devastating malware, ransomware, or both. Luckily, this attack was mitigated.

Following the nearly-successful attack described above, the CISO at the financial institution implemented proactive domain monitoring – including MX-record monitoring.

What could have been different? Lots of things.

The institution had been looking for similar domains previously, but it was a marketing and legal-driven initiative, more focused on trademark integrity, rather than on imminent threat detection and mitigation.

But If they had already implemented security-centric domain and MX record monitoring, the BEC attack emails might never have reached the members of the HR department

BEC and Socially Engineered Attacks Are on the Risk

There is no doubt, criminal attacks using carefully created and carefully targeted emails are on the rise.

The FBI recently reported that global losses related to these Business Email Compromise (BEC) scams experienced a 270% increase from January 2015 to April 2016. These kinds of attacks do real damage.

Billions of dollars have been stolen through these schemes, directly affecting corporate bottom lines.

Sophisticated attacks, like the one described above succeed because they combine three critical elements to create legitimacy....

(1) The "sender" is known and trusted.
(2) The emails are sent to logical recipients
(3) They originate from a seemingly trusted email domain

The most effective attacks originate from a domain that is a close variant of a company's actual email domain. (Instead of XYZ.com, they'll register XYZ.biz, or XYZ-finance.net). Cybersquatters register domains like those every day.

To turn a cybersquatting domain into a spear phishing platform, **a potential phisher activates the domain's MX record. CISOs take note -- the MX record is the key to proactive BEC defenses.**

An MX record is a type of resource record in the Domain Name System that specifies a mail server responsible for sending and accepting email messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available.

An active MX record allows a domain to communicate with other emails domains to send and receive messages. It also can help security professionals predict when an attack may be imminent.

Use MX Records to Proactively Detect Threats

All CISOs who are worried about increased enterprise or institutional risk from spear phishing or BEC attacks should immediately begin monitoring, or engage a partner for proactively monitoring the internet for similar domains, especially for similar domains with active MX records.

In the modern cyber threat world, a rogue domain with an MX-record represents an immediate danger. Frankly, there is only one reason for a criminal to activate the MX record of a copycat domain, or to acquire a similar domain with an active MX record – to attack.

Think of MX records as an early warning system. When CISOs gain intelligence about rogue domains with active MX records, they can take immediate steps to block any email to the enterprise that originates from these possibly dangerous domains.

When an MX record goes active on a similar-looking domain, seconds count. Take decisive action right away. Neutralize these potential attack platforms.

CISOs, you can raise your game when it comes to defending against modern spear phishing attacks. In many cases it makes sense for security teams to take over domain monitoring, integrating domain monitoring, anti-phishing, and other beyond-the-perimeter cyber defense initiatives.

Of course, legal should still be alerted if any similar domains are discovered, because they could still represent a trademark risk.

But by implementing integrated MX-record monitoring, and proactively blocking inbound emails from these potential attack platforms, security is dramatically reducing the enterprises' imminent risks from spear phish or BEC attacks.

About the Author

Dylan Sachs
BrandProtect Services Director, Identity Theft and Anti Phishing

Sachs directs Identity Theft and Anti-Phishing efforts at BrandProtect. He works directly with leading financial institutions, health care providers and Fortune 500 enterprises to help CISOs and security teams deploy better defenses against modern email and identity theft attacks, including socially engineered exploits.

Sachs also leads the Incident Response Team, responsible for developing actionable intelligence on and mitigating the incidents that target our clients.

Yuval Ne'eman Workshop for Science, Technology and Security

ICRC Blavatnik Interdisciplinary Cyber Research Center

אוניברסיטת תל אביב

Prime Minister's Office National Cyber Bureau

2016 CYBERWEEK

June 19th-24th, 2016

Tel Aviv University, Israel

In cooperation with:

Ministry of Foreign Affairs Israel

1 WEEK * 25 EVENTS * 5,000 ATTENDEES

CONFIRMED SPEAKERS INCLUDE:

Caleb Barlow
Vice President
IBM Security

Gil Shwed
Founder, Chairman and Chief Executive Officer, Check Point Software Technologies

Omar Abbosh
Chief Strategy Officer
Accenture

Major Gen. (Ret.) Prof. Isaac Ben-Israel
Conference Chairman
Head of the Blavatnik ICRC, Tel Aviv University

Benjamin Netanyahu
Prime Minister of Israel

Dr. Eviatar Matania
Head of the Israel National Cyber Bureau

Buky Carmeli
Head of the National Cyber Security Authority
Prime Minister's Office

Udi Mokady
Founder, President and Chief Executive Officer, CyberArk

Yoav Andrew Leitersdorf
Managing Partner
YL Ventures

Prof. Susan Landau
Prof. of Cybersecurity Policy Dep. of Social Science and Policy Studies Worcester Polytechnic Institute

John P. Watters
Chairman & CEO, iSIGHT Partners

Michal Blumenstyk-Braverman
GM, Azure Cybersecurity
Microsoft

James Andrew Lewis
Senior Fellow Center for Strategic and International Studies (CSIS)

Alejandro Mayorkas
Deputy Secretary
Homeland Security
USA

Dr. Yaniv Harel
General Manager Cyber Solutions Group of EMC, Head of Research Strategy, Blavatnik ICRC, Tel Aviv University

Mark Gazit
CEO, Theta Ray

Esti Peshin
Director of the Cyber Programs, Israeli Aerospace Industries

Arik Mimran
Vice President
Qualcomm Israel

Chris Roberts
CSH and Senior Consultant
Sentinel Global

Nadav Zafrir
Co-Founder, CEO
Team8

Justin Somaini
Chief Security Officer
SAP

Terry Roberts
Founder and President
Whitehawk

Dr. W. Douglas Maughan
Cyber Security Division Director Homeland Security Advanced Research Projects Agency (HSARPA)

William H. Saito
Special Advisor to the Cabinet & Prime Minister of the Government of Japan

Keren Elazari
Analyst, Author & Researcher, Blavatnik ICRC, Tel Aviv University

Andy Ellis
Chief Security Officer
Akamai

Dr. Kenneth Geers
Cyber Centre Ambassador, NATO

DIAMOND SPONSORS

accenture
High performance. Delivered.

DISTINGUISHED BENEFACTOR

KETER

PLATINUM SPONSORS

Check Point SOFTWARE TECHNOLOGIES LTD.
CYBERARK
EMC² RSA
GE Digital
IAI ISRAEL AEROSPACE INDUSTRIES
IBM
Microsoft
TEAM8
THETARAY
YL VENTURES

GOLD SPONSORS

CYBERBIT PROTECTING A NEW DIMENSION
FireEye
QUALCOMM
REDDOT CAPITAL PARTNERS
TEMASEK
Steven E. Stern
FORCEPOINT

SILVER SPONSORS

IATA
SAP
Telit

In association with

comtec Conventions & Special Events
#BIGIDEA
CYBERTLV
CDM CYBER DEFENSE MAGAZINE
IEEE
Israel Advanced Technology Industries
ISRAEL-BRITAIN CHAMBER OF COMMERCE
ITA ITALIAN TRADE AGENCY
MARKET RESEARCH MEDIA your unfair competitive advantage
Ministry of Foreign Affairs Israel
NOVAWIND BOOSTING BUSINESS
SAGIVTECH
STARTAU

Conference website and free registration: http://cyberweek.tau.ac.il/2016/
Tel: +972-3-6406041 Email: icrc@post.tau.ac.il

It's A Trap! Preparing For Smokescreen DDoS Attacks

Rene Paap, Product Marketing Manager, A10 Networks

The threat landscape is more complex than ever, and establishing a cybersecurity strategy in 2016 entails accounting for a number of different factors. Hackers will employ a variety of techniques to achieve their goals.

In order to establish a viable defense, enterprises and VARs must select the necessary technology for countering different forms of attacks.

One of the most prevalent methods used by cybercriminals is the distributed denial of service (DDoS) attack. This form of attack generates massive amounts of malicious network traffic — usually via networks of infected devices controlled by a single user.

Due to the highly visible repercussions of DDoS attacks, they are carried out for a large number of reasons, including political activism, financial gain, and even ransom. DDoS attacks are becoming an increasingly popular tool in the cybercrime arsenal, and a 2015 Akamai report shows that DDoS attacks increased by 132 percent compared to Q2 2014.

In addition, a 2015 Verisign report found that attack sizes increased by 52 percent from the first to the second quarter, meaning not only are more attacks happening, but they are becoming more severe.

DDoS attacks can range in terms of severity, partially due to the low technical barriers posed to individuals carrying them out. One such popular method is via Web services that allow customers to rent, in a DDoS-as-a-Service manner, the computing power necessary to generate sufficient Web traffic — meaning anyone with a credit card could carry out an attack.

Despite being easy to pull off, DDoS attacks are still employed by the most advanced hackers and cybercriminals. In the right hands, the ability to disrupt a target's networks and bring down critical systems is a means to a larger end, typically a network intrusion.

In these instances, the DDoS attack acts as a smokescreen, diverting IT assets and attention away from typical security processes.

These types of attacks leave the network vulnerable, as it becomes easier to dismiss atypical activity as a false positive, in hopes of buying more time to deal with returning the network to business as usual.

Hackers take advantage of this distraction and in quick succession carry out subsequent attacks, often planting advance persistent threats (APTs) on the network or stealing valuable data.

Since DDoS attacks bring down the most visible part of an organization, namely its website and internal employee Web applications, the pressure put on IT can range from the sales department all the way up to the C-Suite.

A disruption of this sort can lead to lost revenue, a tarnished reputation and a major IT headache through the flooding of IT requests.

The solution for defending against being the victim of a DDoS smokescreen attack is two-pronged. Awareness is key, so organizations must first educate response teams on the various means used by hackers looking to infiltrate the network.

With this knowledge, IT teams can do a better job of determining what the end-goal of attackers is, making it easier to push back against pushy C-Suite executives looking for a quick fix.

The second step of protecting against this sort of threat is technological. Without adequate security solutions in place, IT teams are at a distinct disadvantage when dealing with cybercriminals.

In the case of the smokescreen DDoS attack, a combination of on-premises and cloud-based solutions that incorporate network load-balancing technology can handle attacks of varying types and sizes.

These products give IT decision makers the ability to detect an attack and mitigate it.

Coupled with the appropriate security information and event management (SIEM) solution — and other tools for flagging unusual network activity — organizations can reduce the confusion caused by the initial DDoS attack, while maintaining the diligent monitoring necessary for defending against more serious threats.

About the Author

Rene Paap is a Product Marketing Manager at application networking and security leader *A10 Networks*. Rene specializes in analyzing and educating a product's values, and evangelizing those both inbound and outbound.

Top 10 Ways Healthcare Can Strengthen Security Policy and Better Prevent Cyberattacks

2016 is heading towards setting new records for healthcare cyberattacks and data breaches. North American hospitals hit by cyberattacks so far include Hollywood Presbyterian Medical Center in Hollywood, California; Methodist Hospital in Henderson, Kentucky; Ottawa Hospital in Ottawa, Canada; Mercy Hospital in Iowa City, Iowa; and several hospitals operated by Medstar in Baltimore, Maryland, and Washington, D.C. And this is only the tip of the iceberg.

The nature of these attacks is quite broad. Traditionally, attackers first penetrated hospital networks and then worked silently to exfiltrate valuable patient data. More recently, cyberattackers have used tools such as ransomware, which is designed to produce a quicker profit by directly threatening hospital operations. Until the ransom is paid, these attacks incapacitate hospitals' information technology systems and slow access to critical patient records.

Hospitals are increasingly under attack because of the high value of patient data and the vulnerability of their cyber defenses. Medical records have between 10 to 20 times the value of credit-card data because they generally include complete data on the patient's identity, insurance and credit cards – data that makes it easy to create a false identity. To make matters worse, cyber-defense budgets in hospitals are inadequate; they do not support the talent and technology acquisition necessary to meet the threat head-on.

Hospitals are also plagued by the extreme vulnerability of the medical devices within their networks. Medical devices are closed to endpoint security software or other cyber-defense tools because they are FDA certified. And because these devices often run older operating systems with known vulnerabilities, they create safe harbors where attackers can create "back doors" that standard cyber defenses cannot easily detect. The serious weaknesses that medical devices bring into the security architecture must be dealt with by operations-center personnel.

With cyberattacks on the rise, it is increasingly imperative that the healthcare industry strengthen security policies to better prevent them. New best practices have emerged to help healthcare institutions meet and overcome these threats. The following list outlines the top ten ways hospitals can strengthen security and the best practices that support them.

1. Enhance employee training to help forestall attacks. Attackers commonly enter hospital systems by leveraging the expected behavior of hospital personnel. Two common entry points for attackers are personal email addresses and browsing on the Internet. A large percentage of email contains malware in the form of a URL that either contains malicious attachments or that redirects users to a malware-laden website. Attackers also enter hospital networks by embedding URLs in the text of an email that appears to be from

someone within the organization or whom the employee knows. Sometimes, attackers disguise email as coming from trusted managers in the healthcare organization. The training required for HIPAA compliance provides a good opportunity to make it very clear to employees that the information technology within the hospital environment is not for personal use at any time, under any circumstances.

2. Hire a cybersecurity contractor to perform penetration testing and assessment, which can help hospitals discover and root out cyberattackers. Attackers are probably already within your hospital network, although they may not have been able to steal data yet; they may only be in the early stages of an attack. Experts can find and document many of the vulnerabilities that your current information technology and security operations team can begin to address. Most hospitals have not budgeted for these tests, and they have certainly not budgeted for the costs of a major data breach. This testing is relatively low-cost insurance that can help you understand the risks already inherent within your network.

3. Review and assess medical devices and put an action plan for remediation in place now. Most medical devices cannot be scanned by endpoint cybersecurity and are relatively safe havens for cyberattackers. A remediation plan would note which devices have older embedded operating systems such as Windows® XP or Windows® 7 that are highly vulnerable to attackers and their malware tools.

4. Implement a plan to integrate and deploy the software fixes provided by the manufacturers of your medical devices. Monitor this plan and report on it quarterly to ensure you are making rapid progress towards your goal.

5. Procure medical devices from vendors that focus on cybersecurity processes, encrypt data internally and use other advanced techniques such as white-listing to ensure that files within the system are authorized.

6. Eliminate medical devices that have older architectures, no modern cyber defenses and no viable strategy for dealing with advanced malware such as MEDJACK. Many medical devices have been in service for years, often well beyond their expected life-cycle. Replace outdated devices and acquire new devices with the protection you need from manufacturers that can comply with your requirements.

7. Review existing contracts with medical device vendors, amend them to include support and maintenance, and specifically address the details of malware remediation. Make sure vendors can provide the support you need to investigate the presence of cyberattackers, remediate the problem rapidly and return the device to normal operations status. Medical-device manufacturers should have a documented test process to determine if their devices are infected and a documented standard process to remediate devices when malware and cyberattackers are using them.

8. Tightly manage access to medical devices through their USB ports. Do not allow staff to use USB ports except under conditions and processes approved by your security operations team. One medical device can infect and re-infect the network and open it up to cyberattackers. Since standard cybersecurity suites cannot detect attackers within these devices, do everything possible to minimize access.

9. Isolate medical devices inside a special secure network and isolate this network with internal firewalls that allow access only to specific services and IP addresses. Do not allow general Internet access to these devices under any circumstances. If practical, keep medical devices entirely off any networks that connect to the Internet.

10. Employ new deception technologies designed to identify malware and persistent attack vectors that have already bypassed your primary defenses. Assume that your network has been penetrated and act accordingly. Deception technology automatically deploys camouflaged decoys and lures into the network, where they intermingle with the hospital's real information technology resources. To a cyberattacker, these decoys appear identical in every way to the hospital's real assets, and they are designed to be attractive to attackers moving stealthily within a network in search of high-value assets. The attackers are caught immediately, the moment they touch one of the decoys.

In summary, healthcare networks and hospitals are easy targets for cyberattackers. Healthcare data has high value and remains a target of choice. New best practices and policies can benefit healthcare institutions not only by reducing risk and vulnerability, but also by reducing the time to breach detection when cyberattackers penetrate the security infrastructure.

About the Author

Carl Wright is a seasoned entrepreneur and executive with experience in the security, storage, virtualization and software sectors. Prior to joining TrapX he held executive operational roles at Securify, Decru, and Kidaro, where he contributed to rapid growth and subsequent acquisition by, respectively, Microsoft, Network Appliance, and Secure Computing. He has extensive experience in all aspects of enterprise information technology deployments and has held key IT operational roles, including chief information security officer for the U.S. Marine Corps. He holds a bachelor's degree in management from Augsburg College and a master's degree in information technology management from the Naval Postgraduate School. In 1999, he was awarded the National Security Agency's Frank B. Rowlett Trophy for Worldwide Information Security Professional of the year by General Michael Hayden (U.S. Air Force Ret.).

At CTIA Super Mobility 2016 you'll connect firsthand with the technology, people and ideas driving every aspect of the evolving mobile marketplace and shaping the smart city of tomorrow.

Combining cutting-edge content, keynotes and exhibits alongside interactive "Smart Experiences" that bring the future of mobile to life, CTIA Super Mobility 2016 is now EVERYTHING WIRELESS in one comprehensive, course-charting event.

CTIA Super Mobility 2016 Smart Experiences

- 5G R&D Foundry
- AR/VR Arcade
- Connected Car Lot
- Drone Airfield
- Mobile Health Clinic
- Smart Home
- Smart Office
- Smart Retail Store

ctia Super Mobility 2016™

September 7, 8 & 9, 2016
Sands Expo | Las Vegas, NV

REGISTER NOW CTIASuperMobility2016.com

Cyber Defense Magazine readers receive 20% off! Use promo code: CDM4CTIA

Why Manufacturers Are on the Frontlines of the Next Cyber Battleground

By: Aviv Grafi, CTO and Co-Founder of Votiro

Cyber-security experts – and concerned citizens, including the President of the United States himself – believe that a major cyber attack on critical infrastructure in the US is just a matter of time.

Sooner or later, a hacker is going to send out the "right" kind of spear-phishing message that someone at an electricity provider or a water infrastructure firm is going to click on, spreading malware that will shut down the power, poison the water, or otherwise cause pain, suffering, or even worse to millions of people.

But critical infrastructure systems – controlled by SCADA systems and legacy software and hardware – are hard to get at, because those systems are usually kept separate from data networks where users are likely to click on links or attachments that hackers use to spread their poison.

As was the case with Stuxnet (or so the story goes), you usually need to physically access a critical infrastructure system in order to take it over.

Although there are always exceptions, the difficulty in reaching those systems may be one reason why we have not seen the rash of infrastructure attacks that the experts have been expecting.

But what if hackers were to target a manufacturing infrastructure system? Instead of taking a chance that the victim of a spear-phishing attack will take the right steps – access a targeted server, or take another required action – to allow their malware to hit power plant or water filtration systems, hackers could get a lot more mileage out of a spear-phishing campaign at a factory that manufactures, for example, brakes for vehicles.

Since the data and administrative networks and the manufacturing systems are well-integrated in such places, hackers would be able to much more easily compromise a manufacturing plant than a critical infrastructure site.

Possibly the headlines wouldn't be as big, but the damage could be enormous, and the hackers – cyber-criminals or cyber-terrorists – could much more readily achieve their goals.

If, for example, hackers were able to get access to a system that calibrates the brakes that go into new cars – changing the shape or size of a disc so that it does not meet standards – they could wreak havoc, by either keeping quiet while brakes are installed in vehicles (with the attendant tragic results) or extort the company for millions, by withholding information about batches of bad brakes that were shipped, potentially exposing the manufacturer to millions in lawsuits.

Apply that scenario to manufacturers of airplane parts, nuclear powerplant parts, water pipes, MRI equipment parts and so on, and the magnitude of the problem we are facing becomes all too clear.

Many companies rely on traditional solutions, such as sandboxes, to prevent cyber attacks. By scanning an email in a sandbox environment, where they are checked for malicious activity, organizations believe they can keep their users away from malware.

But as usual, the hackers have gotten the upper hand; almost all malware available today can – and has successfully – evaded sandbox protection.

Naturally, sandbox evasion presents problems for companies and users alike: hackers have found way to bypass security solutions and access private, vital information.

"Zero day exploits," present an even more troublesome danger for cybersecurity experts because no security solution can prevent or detect them.

And while not every hacker is skillful enough to come up with a zero day exploit, they can easily purchase a fully functional zero-day or undisclosed exploit on the Darknet.

Clearly, advancements in cyber attacks, such as advanced sandbox evasion techniques, call for a new approach, one that can protect from undisclosed exploits and remain immune to future attacks.

One such approach that Gartner makes mention of is the use of content disarm and reconstruction (CDR) at the email gateway as a supplement or alternative to sandboxing.

The most pressing place for these changes to take place is within the institutions that affect us the most: critical infrastructure and manufacturing.

Last October, President Obama rightly termed critical infrastructure safety a matter of national security, and called on officials in business and industry – especially those responsible for critical infrastructure – to shore up their defenses.

But that message needs to be heard by manufacturers, as well. It's encouraging that critical infrastructure defense is now on the radar of the President and many others, but defending manufacturing infrastructure must also be addressed– as soon as possible.

What to do? Of course, educating employees not to open suspicious attachments is always important – but according to an end-of-year report by ICS-CERT, an astounding 91% of hack attacks utilize spear-phishing tactics.

Clearly, either the education we have been imparting has not been working, or the hackers are now so adept at psychological manipulation that it is almost impossible for the average worker – even the tech-savvy ones – to avoid.

Part of the solution lies in raising the profile of cyber-security in this industry. In many companies, cyber is seen as the duty of IT staff. Unfortunately, many IT people don't have the up-to-date knowledge needed to prevent hacking.

“Standard” solutions – sandboxes, anti-virus software, and even firewalls – are outmoded, as hackers have figured out end-runs around them.

Cyber-security tech firms have new solutions that can help prevent hacking and spear-phishing attacks – but learning about those solutions, figuring out which ones are appropriate, and implementing and managing them is a full-time job.

All companies – and especially manufacturers - that want to protect themselves need to hire a professional cyber-security manager at the very least or, preferably, a seasoned CISO who can be sure to match the right security solutions to the right threat.

President Obama himself realizes this; part of his Cybersecurity National Action Plan entails hiring a full-time Federal Chief Information Security Officer, “to drive cybersecurity policy, planning, and implementation across the Federal Government,” according to the White House announcement.

Managers, factory owners – and any other company that is concerned over losses due to increasing levels of hacking – would do well to follow his example.

About the Author

Aviv Grafi is the CTO and Co-Founder of Votiro. He has over 10 years of experience in the fields of telecommunications, embedded technologies, and information security. Prior to co-founding Votiro, Aviv served in an elite intelligence unit of the Israeli Army. Aviv holds a B.Sc. in computer science, a B.A. in economics, and an M.B.A. from Tel Aviv University.

He is the inventor and principal software architect of Votiro’s enterprise protection solutions. Aviv can be reached by email at aviv@votiro.com or on the company’s website at www.votiro.com.

TCCA
TETRA - Critical Communications Association

Presents

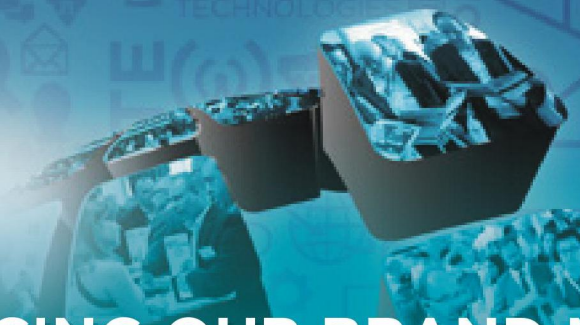
31 May - 2 June 2016
RAI Amsterdam

18th Annual

CRITICAL COMMUNICATIONS WORLD

INCORPORATING:
TETRA WORLD CONGRESS

DEVELOPING CRITICAL COMMUNICATIONS IN A NEW ERA OF DATA, APPLICATIONS AND EMERGING TECHNOLOGIES



INTRODUCING OUR BRAND NEW ZONES

DATA APPLICATIONS & CONTROL ROOMS

CYBER SECURITY

FUTURE TECHNOLOGIES

GOLD SPONSORS:

AIRBUS DEFENCE & SPACE
HUAWEI
LEONARDO
MOTOROLA SOLUTIONS
ROHILL
sepura

MISSION CRITICAL OPERATOR:

bravo Enterprise communication

SILVER SPONSORS:

Bittium
COBHAM
DAMM
ERICSSON
GENERAL DYNAMICS Mission Systems

ENDORSED BY:

3GPP A GLOBAL INITIATIVE
ETSI World Class Standards

www.criticalcommunicationsworld.com

Produced and researched by: IIR TELECOMS & TECHNOLOGY www.iir-telecoms.com

Patients, Data and Mobile Medical Devices – How to Protect Them Against Malicious Attacks

A slew of revolutionary Internet-connected portable medical devices are beginning to disrupt the Healthcare industry in radical ways. As a result, the way patients manage their health, communicate with doctors and monitor their activity levels has opened the door to new methods of prevention, but more importantly, promises to help in the treatment of chronic diseases.

Health consciousness among people across the world, increasing chronic diseases such as diabetes, and growing healthcare expenditure, is driving the growth of this potentially vast market for wearable, or portable, medical devices.

According to a report entitled "Portable Medical Devices Market" by Market&Markets, the total Portable Medical Devices market is expected to cross $20 billion by 2018, growing at a double digit rate each year.

Analysts, however, expect the medical device market to see major headwinds such as high costs for the development and deployment of consumer healthcare and mobile medical devices, strict government regulations and all kinds of nightmarish data security and privacy issues.

There are two primary classes of portable medical devices – consumer devices that generally support lifestyle and prevention, such as FitBit, Apple Watch and so on, and connected devices that monitor and in some cases administer treatment such as heart monitoring halters, implantable insulin pumps and sleep devices. Over the next 20 years, the kind of device is limited only by the human imagination.

These devices typically transmit sensitive data and control signals to an app on a mobile device like a smart phone. In addition to containing highly sensitive personal information, the control signals can affect the functioning of the device. With this connectivity, the potential for data misappropriation, malware, or worse, will intensify, especially where mobile apps are concerned.

While a manufacturer has the luxury of employing specialized hardware and software to secure the actual device, the mobile app, residing on an operating system such as Android, represents an often weakly defended backdoor to an otherwise secure system.

According to the Identity Threat Resource Center, the U.S. healthcare/medical industry saw 112.8 million records breached in 2015 – by far the most of any industry. This translates into roughly one in every three Americans that became a victim of a healthcare breach. While these attacks were typically on well-protected, enterprise-level health records, this trend does not bode well in an age of billions of poorly protected mobile devices.

As mobile and wellness devices and the apps associated with them become ubiquitous, bad actors will naturally turn to these devices and apps as a prime target. Given the sensitivity of the

data being handled, security and privacy must become a priority. The critical question is: how can device manufacturers and app developers reduce the potential for data leaks?

As the demand for mobile medical devices and healthcare apps grows, the need for next-generation tools that protect and detect application and data security vulnerabilities are a must.

In fact, already in 2014 the FDA released a guidance document containing nonbinding recommendations for the management of cybersecurity devices, which states cybersecurity risk management is a shared responsibility among stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices.

The FDA also states that the failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. Manufacturers must address cybersecurity from the start, during the design and development stages of their medical device, as this results in more robust and efficient mitigation of patient risks; they must also focus on every aspect of the data path, not just on securing the actual device, but also the software-based apps that talk to the device.

The loss of data resulting from malware is a typical threat that an application needs to withstand. A hack can go way beyond impacting privacy, ruining corporate reputations and impacting the bottom line – in this case, a hack can literally kill someone. In short, mobile medical apps and associated devices that are regulated by the FDA also need to maintain their integrity and should not depart from its specific prescribed behavior.

To lower the risk of malicious attacks and unwanted alterations of sensitive mobile apps running in unmanaged environments, software protection best practices need to be established.

Best practices and security methods that have been used for the protection of software applications in other industries such as Finance, Automotive and Media need to be adapted and then adopted to prevent security breaches in the Healthcare industry and protect patient data.

Today, the U.S. FDA [1, 2] publishes nonbinding recommendations for the management of cybersecurity for medical devices, which include the following security-related recommendations:

1. Limit access to devices through the authentication of users, limit access to trusted users only.
2. Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.
3. Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.
4. Employ appropriate software/hardware protections against malicious observation/modification of medical device secrets by the device possessor.

5. Avoid unauthorized access or deliberate modification of application generated and/or managed data by a malicious device owner.

Manufacturers have a series of options at their disposal to achieve the required level of cybersecurity. The use of these tools is highly recommended in case the hardening of particularly sensitive and critical customer facing apps is a must.

Access control, user authentication, the encryption of data in transit and at rest, and a secure software update and maintenance process can be achieved by using secure implementations of standard cryptographic algorithms and secure systems best practices.

However, protecting apps and other software running in open operating systems while it is running poses new problems – attackers have developed reverse engineering techniques based on debugging and other technologies that allow them to expropriate secrets while the app is running.

To protect systems against these attacks, developers must employ software tamper resistance techniques such as white box cryptography and code hardening. These techniques provide apps with a "self-defense" capability even when running by keeping cryptographic keys that are used for encrypting and decrypting data or for user authentication purposes persistently protected at rest and during execution of the application.

Device makers and solution providers can achieve a high level of software based security by using white box cryptography in combination with hardening software application on source code level. These application hardening tools, also known as code protection tools, can prevent reverse engineering and other techniques used by cyber-criminals who attempt to gain access to sensitive information and resources contained in the software applications.

These tools work at the source code level, obfuscate source code, and make it more difficult for attackers to review the code and analyze the application. They also implement integrity checks, which can deter manipulation and deliberate modification of the app, and code lifting.

But state-of-the-art software security solutions not only focus on obfuscation at the source code level and application integrity, but also provide a high level of threat protection.

Threat protection adds functions to the mobile medical app to detect and/or prevent the app from being run on rooted or jailbroken devices, in emulators, in debuggers or when code has been tampered with, like having been instrumented with debug code or repackaged with malicious code.

So each additional security measure increases the security level on a sensitive app, but only the combination of code protection and white-box cryptography with threat protection functionality will achieve the highest level of software security.

Medical devices and wellness apps will only increase in use, and with this comes a plethora of security and privacy issues. We have already seen this with ransomware attacks in healthcare

facilities, and they come at a cost, not just to reputation but also to the bottom line. Tackling device and application security is a crucial step toward protecting not only healthcare facilities but the patient data on which they depend. The good news is that cost efficient, easy to use software-based security solutions are available today and hardened software apps are already broadly deployed in other industries. So this is not a proof of concept, but a call for action.

About the Author

Thorsten Held, *Managing Director*

Thorsten Held is a co-founder of whiteCryption and rejoined the company in January 2014 as Managing Director leading all global operations. Currently he is responsible for driving growth and ensuring high satisfaction among whiteCryption customers.

With more than 20 years of experience in the Software and Information Technology industry as an experienced business development executive, he spent 5 years with Teleplan International, a leading provider of service solutions for A-brand customers in the Computer and Communications industry. During his career, he has also spent time on the buyer's side of software security solutions at Steinberg Media Technologies where he was head of product development. In addition to this, he has held several leadership positions in fast growing IT companies, including Syncrosoft, the predecessor of whiteCryption, where he drove sales and the licensing of one of the most secure software copy protection solutions.

Held holds a Diploma in Electrical Engineering from the University of Applied Science in Hamburg, Germany.

FDA sources:

1. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

2. Mobile Medical Applications
Guidance for Industry and Food and Drug Administration Staff

Document issued on February 9, 2015.

(ISC)²

SECURITY CONGRESS

APAC 2016

25 - 26 July · Centara Grand CentralWorld · Bangkok,Thailand

ADVANCING SECURITY LEADERS

Join (ISC)² for 2 days of insightful discourse and a post-congress technical workshop as top-notch InfoSec luminaries representing academia, government and industry from Americas and Asia discuss emerging threats, best practices, and solutions to challenges.

EARLY BIRD REGISTRATION

Register Now - Deadline: May 31

Early Bird Price: USD $255 | Standard 2-Day Pass: USD $300

30+ International Speakers

2 Days

6 Tracks

30 Sessions

- Keynote Presentations
- Interactive Sessions
- Regional Roundtable Discussion with information security experts
- Post-Congress Technical Workshop

Tracks Include:

- Cloud Computing
- Critical National Information Infrastructure & Industrial Control System (ICS)
- Government & Law Enforcement
- Mobile Device Management & Internet of Things (IoT)
- Security, Sustainability & Integrity
- Student Track

Sponsors:

Hewlett Packard Enterprise

ssh communications security

In partnership with: image engine

For Inquiries: (852) 2850 6953
securitycongressapac@isc2.org

Visit apaccongress.isc2.org

#ISC2congressAPAC

How Banks, Other Businesses Can Avoid Becoming Cyber-Crime Victims

Apparently, the heist couldn't have been any simpler if it had been drawn up in the lunch line at an elementary school cafeteria.

In February, Bangladesh's central bank saw $81 million disappear out a virtual window. Now it's been revealed that, although the computer hackers used custom-made malware, they probably didn't need to work up a cyber sweat while pulling off their long-distance theft.

The bank had no firewalls to defend against intruders and its computers were linked to global-financial networks through second-hand routers that cost $10.

"It's stunning that a major institution would leave itself so defenseless in this day and age when everyone should know that cyber criminals are waiting for you to let your guard down," says Gary S. Miliefsky, CEO of SnoopWall (www.snoopwall.com), a company that specializes in cyber security.

But he says the episode can serve as a cautionary tale for other banks and any businesses that want to protect themselves against today's cyber versions of Bonnie and Clyde.

"Most companies have some vulnerability and it doesn't take a sophisticated attack to cause a security breach," Miliefsky says. "Often on the hackers' end of things, it just takes patience."

For example, he says, a cyber criminal can gain access by sending a company an email with an attachment called a Remote Access Trojan, or RAT, that looks like a normal file.

All it takes is for an unsuspecting employee to open that file and, voila, security is compromised.

That's bad for companies, of course, but it's also bad for consumers, whose bank account, credit card and other private information is at risk.

Miliefsky says it's important to go on the offensive. Among his recommendations:

• Employers need to train their staffs.
Those employees sitting at their computers each day are a company's first line of defense. An errant click on the wrong email is like unlocking the front door, so employees should be made aware of the dangers and told what do about suspicious email.

• Companies should routinely update their defenses.
Outdated technology and outdated security software make a company's computers vulnerable

to attack. It's important that businesses periodically review their IT operations to make sure what worked last year still provides the needed security.

• Consumers must take their own safety measures.
It would be nice to expect banks and retailers to protect consumer information, but the average person can't count on that. Miliefsky suggests consumers take personal security measures such as frequently changing passwords and deleting any phone apps they don't use. Many apps contain malware that can spy on you.

"Most people log onto the internet every day without much thought about how susceptible they are to being hacked," Miliefsky says. "It takes vigilance to protect yourself against cyber criminals who are working hard to figure their way around security measures."

About Gary S. Miliefsky

Gary S. Miliefsky is founder of SnoopWall Inc. (www.snoopwall.com), a cutting edge counter-intelligence technology company offering free consumer-based software to secure personal data on cell-phones and tablets, while generating revenues helping banks and government agencies secure their networks. He has been active in the INFOSEC arena, as the Executive Producer of Cyber Defense Magazine and a regular contributor to Hakin9 Magazine.

2 Step Authentication vs 2 Step Verification

We often get the option of using more than one factors for authentication to verify our identity for an account. Using ATM card is a good example of that. We provide a PIN and the ATM card to authenticate ourselves to the Bank. This is called **2 Step Authentication**.

Again, sometimes we use One Time Password or OTP to login in an account. For example, while using Gmail we often get the option of authenticating ourselves using a password as well as an SMS sent over to our mobile. It is often called **2 Step Verification**.

We often use the terms 2 Step Authentication and 2 Step Verification interchangeably. Are they same or are they different ? How are they different from each other ?

Let's understand first what 2 Step Authentication and 2 Step Verification actually are.

Authentication factor is the different credentials that a user use to verify her identity. These factors can be of three types :

- Knowledge factors, i.e. something the user knows, such as passwords, PIN or any pattern.
- Possession factors, i.e. something the user has, such as ATM cards, phones etc.
- Inherence factors, i.e. something you are, for example biometric like fingerprint, eyeris etc.

In a **2 Step Authentication**, the user uses any two types of the above factors, for example PIN and ATM card, password and biometric etc.

In a **single factor authentication**, the user uses only one type of credentials, a password for example. Most online accounts support single factor authentication.

But as we know, single factor authentication is not secure enough. For an online account that supports passwords only, can easily be hacked by attackers using various malicious methods. And thus, we needed a 2 Step Authentication procedure.

2 Step Authentication process support two types of credentials. So, even if one of the credentials of a user gets compromised, the account still remains safe, as long as the second credential of the particular user is not hacked by the attacker.

As I said, a good example of 2 Step Authentication can be authentication using ATM card and PIN.

Even if the user's PIN is compromised, the attackers cannot hack the account as long as they are unable to physically possess the ATM card of the user.

And thus, 2 Step Authentication using PIN and ATM card is, in fact, considered to be widely successful authentication process.

Recently, many online accounts like that of Gmail also use two types of credentials from the user. Usually, a password along with a One Time Password is used as two credentials. And, we call it **2 Step Verification**.

If we think about the security perspective, 2 Step Verification cannot be considered as safe as 2 Step Authentication. Just to give a simple example, a hacker can hack the password of a user using various malicious methods and at the same time, also use attacks like Man-In-The-Middle Attack to steal the One Time Password coming to the user's mobile.

One Time Passwords normally come to a mobile using an SMS or an automated phone call to the mobile. So, an attacker can intercept the SMS or phone call by using various nefarious methods and steal both the credentials.

Even One Time Passwords over emails are also not secure enough for similar reasons.

So, though mobile phones are considered to be something that the user possesses, the One Time Password received in it is something that can be known by the attacker without physially stealing the device. And hence, 2 Step Verification is not same as 2 Step Authentication.

And as discussed above, in terms of security, 2 Step Authentication is much more secure than 2 Step Verification.

About the Author

Amrita Mitra is a Cyber Security Researcher and an enthusiast of Mathematics. Her researches include recent threats and their defenses and detection of various cyber attacks. She also enjoyes learning about PGP.

Amrita maintains her blog site computersecuritypgp.blogspot.com which is dedicated towards increasing Cyber Security awareness among people.

Executive Guarantor

AFCEA

In cooperation with

Future of Cyber Conference 2016

CYBER TRENDS

3rd edition of Future Cyber Security & Defence Conference

General Partner

Deloitte.

Conference Partners

Microsoft · Fidelis Cybersecurity · CYBERGYM EUROPE EXPECT THE UNEXPECTED · net pointers communications

20 – 21 OCTOBER 2016

PVA EXPO PRAGUE, Czech Republic

Cyber Threats & Trends 20 OCTOBER 2016

Cyber Education 20 OCTOBER 2016

Cyber/Hybrid Warfare 21 OCTOBER 2016

Cloud Security 21 OCTOBER 2016

and

- SIX accompanying CYBER WORKSHOPS
- CYBER PAVILION TableTop Presentations

Conference Patronage & Support, Honorary Chairmen:

Mr. Dušan NAVRÁTIL, Director, National Security Authority, Czech Republic

Mr. Milan CHOVANEC, Minister of Interior, Czech Republic

Mr. Martin STROPNICKÝ, Minister of Defence, Czech Republic

MGen. Erich STAUDACHER Deputy Director of the Bundeswehr Planning Office, Germany

BGen. Prof. Bohuslav PŘIKRYL Rector, University of Defence, Czech Republic

Assoc. Prof. Jozef PUTTERA Rector, Armed Forces Academy of General Milan Rastislav Štefánik, Slovakia

Assoc. Prof. Josef SALAČ Rector, Police Academy Prague, Czech Republic

Mr. Petr JIRÁSEK Chairman, AFCEA Czech Cyber Security Working Group, Czech Republic

Assoc. Prof. Lucia Kurilovská Rector, Academy of the Police Force in Bratislava, Slovakia

Conference is a part of:

FUTURE FORCES FORUM

International Platform for Trends & Technologies in Defence & Security

POLICY - DIPLOMACY - DEFENCE - SECURITY - R&D - ACADEMIA - INDUSTRY

General Partner

LOM PRAHA

General R&D Partner

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Partner

VOP CZ

Future Forces Exhibition, 19 – 21 October 2016
World CBRN & Medical Congress, 19 – 21 October 2016
Future Soldier Systems Conference, 20 – 21 October 2016
Military Advanced Robotic Systems Conference, 20 – 21 October 2016
Geospatial, Hydro meteorological and GNSS Workshop, 19 – 21 October 2016
Logistics Capability Workshop, 19 – 21 October 2016
CBRN Workshop, 19 – 21 October 2016
Medical Workshop, 19 – 21 October 2016

www.future-forces-forum.org

THE TOP TEN MOST OUTRAGEOUS HACKS OF ALL TIME

10

CLIMATEGATE

WHAT HAPPENED?

Thousands of emails and computer files taken from the Climatic Research United at University of East Anglia.

These emails were reported to contain evidence that global warming was a conspiracy.

Nov 2009

STATS

Did They Really?

No.

No. eMails & Documents Stolen:

3,000+

No. Scientists Convinced:

0

9

US DEFENCE

WHAT HAPPENED?

Hacker Jonathan James successfully committed perhaps the number one entry on any hacker's wish-list when he infiltrated the US Department of Defence (DoD).

He was arrested, convicted and placed under house arrest – the first juvenile incarcerated for computer hacking.

Jun 1999

STATS

His Age at DoD Attack:

15

Length of Sentence:

6 Months

Sentence if Adult:

10+ Years

READ ON FOR 8-6...

BURGER KING

8

WHAT HAPPENED?

Burger King's twitter profile was hacked supposedly by a group affiliated with Anonymous.

The profile was re-named 'McDonalds' and began tweeted pro-McDonalds messages as well as retweeting complaints about Burger King.

Feb 2013

STATS

What Did They Tweet?

"We just got sold to McDonalds! "

Account Infiltrated:

1h 45m

Followers Gained:

300,000+

WHITE HOUSE

7

WHAT HAPPENED?

Advanced cyber-attacks hit the White House in April 2015. Though the documents that were stolen were relatively minor and not classified it was still a huge source of embarrassment to the Secret Service.

Apr 2015

STATS

What Did They Hack?

President Obama's schedule & various unclassified documents

Who Was Responsible?

Unconfirmed, although some sources suggest Russia

eBay

6

WHAT HAPPENED?

Sometime around late February and early March 2014, eBay's database was hacked and millions of user details and encrypted passwords were stolen.

While this is a relatively standard hack, it's the number of users who were affected that make it so outrageous.

Feb 2014

STATS

Accounts Compromised:

145 million

Method of Entry?

Employee login details

READ ON FOR 5-3...

5

UNITED NATIONS

WHAT HAPPENED?

Not even the United Nations is safe from hackers.In 2014, a pro-Palestine hacking group breeched the United Nations website vandalising it with their logo & messages in support of the Palestinian cause.

Dec 2014

STATS

Group Responsible?

AnonGhost

No. Gov Websites Hacked:

120+

4

PLAYSTATION

WHAT HAPPENED?

PlayStation Network services started to deteriorate over two days, before Sony was forced to suspended its Network entirely. The whole episode was scandalous and they really struggled to repair the damages.

As a result, Sony was fined £250,000 by the British government for having a system so poor it did not even comply with British law.

Apr 2011

STATS

Network Down Time:

23 Days

Account Details Stolen:

77 Million

Estimated Cost to Sony:

£119 Million

3

KEVIN POULSEN

WHAT HAPPENED?

Californian radio station KIIS-FM ran a competition to give away a Porsche 944 S2 to the 102nd caller after a certain set of songs. Michael B Peters was the lucky man who got through, winning the car and collecting his prize.

However, it was later discovered that Michael B Peters was in fact infamous hacker Kevin Poulsen who had broken in to the radio's phone system and rigged the result so he would win.

Sept 1993

STATS

Hack Worth:

£59,000

Other Kevin Poulsen Hacks:

FBI, US Army, His Own Trial

Where is Poulsen Now?

Contributing Editor at Wired

READ ON FOR 2-1...

2

Oct 2011

SESAME STREET

WHAT HAPPENED?

In 2011 an unidentified hacker took control of Sesame Street's YouTube channel and began posting videos with pornographic content.

The hackers posted a comment saying "Who doesn't love porn, kids? Right! Everyone loves it!"

STATS

Content Online for:
22 Minutes

Channel Subscribers:
140,000

1

Dec 2014

THE INTERVIEW

WHAT HAPPENED?

In 2014, Sony Pictures were gearing up to release The Interview, in characters attempt to assassinate Kim Jong Un, the leader of North Korea. North Korea's government branded it 'an act of terrorism'.

They hacked Sony's corporate network, stole private data and threatened further attacks if Sony released the film.

STATS

Personal Records Stolen:
47,000

Cost to Sony?
£10.5 Million

Follow Up Attacks:
0

THE TOP TEN MOST OUTRAGEOUS HACKS OF ALL TIME

REDSCAN™

CONTINUOUS DETECTION AND RESPONSE

Securing the Future of Everything Wireless

By: Heather Lee, Show Director & Conventions AVP

For cybersecurity professionals, asking "What's the next big thing?" is like asking "What's the next big security risk?" IoT, Bring Your Own Device (BYOD), mobile malware, use of company devices on insecure Wi-Fi hot spots and other advances in technology are rapidly changing the cyber defense industry as we know it.

By 2020, Gartner predicts that more than 25 percent of identified attacks in enterprises will involve IoT—but IoT will account for less than 10 percent of IT security budgets. The added security risks that accompany our increasingly mobile working world must be addressed quickly and efficiently for these innovations to be a benefit, rather than a burden, to organizations. IT departments must keep up to date on the security implications of mobile and connected technology in tandem with the process of adopting them into their enterprise.

To stay up to date with the latest security strategies for IoT and everything wireless, thousands of attendees from the wireless industry will gather in September at CTIA Super Mobility 2016 to acquire vital information on new technologies, issues and practices by attending the CTIA Mobile Intelligence Conference.

The CTIA Mobile Intelligence Conference is an open-dialogue program designed to propel the wireless industry forward. These educational sessions will allow attendees to stay abreast of crucial technical intelligence, best business practices and the key issues in cybersecurity for the next generation of wireless technology.

As part of the CTIA Mobile Intelligence Conference's **Everything Connected: Smart City + Smart Consumer** track, speakers will tackle issues surrounding consumer privacy and data security and how these impact the evolution of 5G services and applications.

In the session "Securing the Foundation of A 5G World: Establishing a Framework for Cybersecurity that Enables IoT," attendees will learn how cyberattacks on U.S. businesses and their communications networks are a part of today's digital economy, as much a part of doing business in the mobile broadband marketplace as deploying spectrum.

The **Everything Enterprise: 5G Use Cases** track will focus on the evolving approach to cybersecurity solutions. The "Cybersecurity: Understanding the Ecosystem" session will examine mobile cybersecurity as a team sport where all ecosystem players—carriers, manufacturers, applications developers, stores and platform providers among others—must work together to protect an open ecosystem in which cyber threats have grown and become increasingly sophisticated.

A key theme for this track will be how the openness and global reach of the wireless internet requires flexibility, information sharing, collaboration and vigilance as well as the importance of

the mobile industry players to monitor and share information about cyberthreats and effective countermeasures.

Back by popular demand is our **Everything Policy: How Washington Shapes Mobile** track, which will explore how government actions in cybersecurity and privacy can shape how the mobile broadband sector evolves in the U.S. You'll hear directly from the key government leaders responsible for cybersecurity. In the session "A New Paradigm for Cybersecurity: Partnership v. Regulation," attendees can hear more about the 2014 White House announcement of a National Cybersecurity Framework developed by NIST in collaboration with industry.

This session will explore the changes the Framework has driven in paradigm toward a flexible industry-government partnership to address cyberthreats to critical infrastructure, and its ability to bring together all the key players as a team to respond to an ever-changing threat environment.

During this session, government cybersecurity executives will sit down for an in-depth discussion about the issues surrounding mobile cybersecurity under the NIST Framework.

You need to attend CTIA Super Mobility 2016 in Las Vegas, September 7-9 to stay ahead of the curve on security for everything wireless.

SpyEye Sentencing

Malware Author and Co-conspirator Receive Hefty Sentences in SpyEye Cybercrime Case

On Wednesday, April 20, 2016, a federal judge handed down stiff sentences for Aleksandr Panin ("Gribodemon" or "Harderman"), author of the infamous SpyEye banking trojan, and his co-conspirator, Hamza Bendelladj ("bx1"). Because both co-defendants pled guilty, there was no actual trial. What followed instead was described by seasoned attorneys on both sides as the "weirdest" sentencing hearing they had ever witnessed.

The SpyEye Conspiracy

Panin developed SpyEye and began offering the kit or sale on underground cybercrime forums in 2010, marketing it with the tagline "ZeuS Killer". Bendelladj was not just one of Panin's two main customers, but partnered with him and developed plugins for SpyEye, including the "spreader" plugin and the "ATS" (automated transfer system) plugin that helped bring SpyEye up to feature parity with ZeuS. Both men were prosecuted as conspirators in the same cybercrime case.

Bendelladj, a citizen of Algeria, was arrested in early February 2013 by authorities in Thailand working in conjunction with the FBI. He was nabbed at the airport in Bangkok as he traveled from his home in Malaysia to vacation in Egypt.

Panin was arrested on July 1, 2013, as he flew through Atlanta's Hartsfield-Jackson airport on his way back to Russia from a vacation in the Dominican Republic. The third individual in the main SpyEye triad, James Bayliss ("Jam3s" or "Jam3s2k"), a British citizen, was arrested in May 2014 is being prosecuted by UK authorities.

"Weird" Sentencing Hearing

Both Panin and Bendelladj pled guilty in US federal court. Panin entered into a plea deal which, although it drastically limited his options to appeal, also capped the losses for which he would be held responsible and which determine his sentence. Bendelladj, however, plead guilty without the benefit of a plea deal, and could still appeal his sentence.

Initially, the sentencing hearing was delayed because of a change in venue from New York to Atlanta, Georgia. The discovery of a command-and-control (C2) server in Atlanta, which was operated by Bendelladj, and the discovery of several victims in Georgia gave the Northern District of Georgia jurisdiction in the case.

Sentencing hearings in the same court are sometimes scheduled in 30 minute blocks. These are often for large, complex, federal crimes cases. They rarely take more than a day, even with without plea deals which would take much of the guesswork out of the sentencing.

Because Bendelladj's strategy for a reduced sentence hinged on the actual number of unique stolen "access devices" (a physical thing or data, like a credit card, that can be used to access an account), and the differences in each side's totals were hotly contested, the sentencing hearing became a sort of trial all its own.

The sentencing hearing alone lasted five full days over March and April 2016. Witnesses were called on both sides. Extensive testimony was given. There several lengthy rounds of direct examination, cross-examination, and redirect.

Dozens of exhibits ranging from brief affidavits to detailed forensics reports were entered into the record, often with objections that had to be argued. What made it seem odd to anyone familiar to court proceedings was that issues normally thought of being trial issues were being argued under the very different evidentiary and other rules of a sentencing hearing.

Key Evidentiary Factors in Sentencing

The sentencing guidelines used in US courts for economic crimes apply to these types of cybercrime cases. In this case, the guidelines suggest sentences based on two main types of harm caused:

1. Harm caused to victims of SpyEye infections, including damage to computer systems and remediation costs
2. Harm caused to financial institutions and their customers through the theft, use, and resale of account "access devices" such as credit card "fullz" containing personal and financial information obtained through the use of SpyEye and related hacking activity

Both are still the result of gaining unauthorized access to a computer system, federal felony violations.

Harm Caused by Infection

In the first instance, the following were debated:

- The total number of infections vs. the number of "encounters" in a given timeframe
- The effectiveness of anti-virus software in both detection/prevention and removal roles
- The impact of the availability of free or bundled anti-virus software on average remediation costs

- How many infections could be attributed to each of the separate co-defendants vs. other SpyEye customers

The harm here would be calculated by the total number of infections for which each co-defendant was found responsible times an average remediation cost. The prosecution produced a range of costs. The defense argued that anti-virus software was freely available and already bundled with and automatically updated on virtually all PCs.

The defense argued that this free anti-virus software, as long as it was "allowed to run", would prevent SpyEye infections, and if any existing infections were found, it would be 100% effective in restoring the system to its pre-infection state at zero cost to the user. In the end, the judge accepted the lowest figure in the range quoted by the prosecution.

Harm Attributed to Stolen Data

In the second instance, the following issues were argued:

- How many "access devices" were discovered in each co-defendant's possession
- The average financial harm attributed to a stolen access device
- What constitutes an access device
- Factors that might influence the financial harm attributed to the theft of an access device

The court guidelines are clear that USD $500 is to be considered the average financial harm attributed to stolen access devices. The bulk of the testimony involved how many incomplete or duplicate records existed in the evidence recovered from the various computers and external hard drives that were in in Bendelladj's possession when he was arrested.

This was the subject of multiple rounds of lengthy witness examination and the biggest contributor to the "highly unusual" five-day length of the hearing. At one point, an expert witness for Bendelladj's defense team spent quite some time setting up a Raspberry Pi and projecting the connected LCD panel's output onto a screen just to run the "grep" and "comm" Linux commands a single time each.

To be fair, the numbers produced would form the facts that directly correlated with how many months Bendelladj would be sentenced to spend in a federal prison.

On the other points, some records contained personal customer information, but no credit card number, some lacked CVV2 codes, and others had card expiration dates that had passed.

Payment card data lacking these details may not seem very useful, and indeed they sell for far less in underground markets, but "carders" can use the information to get cads reissued, use criminal-to-criminal (C2C) services to fill in missing details, and find other ways to monetize records with these missing bits.

While hundreds of thousands of records that appeared to be bank accounts of French citizens were thrown out, the court adhered to the $500 guideline and split the discrepancy between the two opposing parties' totals equitably.

Other Key Factors in Sentencing

Other factors that played a key role in determining sentences in this case were the degree to which each of the co-defendants cooperated with authorities and the concept of deterrence.

Cooperation

Panin, by all accounts, cooperated fully with authorities from the second he was arrested, and he appears to continue to do so. For the most part, Panin and his counsel sat passively throughout the hearing, his fate practically predetermined by his plea deal. Panin's attorney did give a closing statement, but it was Panin's own statement at the end that was more compelling.

From the pale-skinned, eyeglasses-wearing programmer in a baggy orange jumpsuit and ankle shackles came a deep, measured voice in a heavy Russian accent.

With eyes closed, it would be difficult to tell Panin's voice from that of the villain Bane in the *Dark Knight* trilogy of Batman movies. The statement Panin gave, however, was one of unqualified remorse, making no excuses, accepting full responsibility, and professing trust in the fairness of whatever sentence the judge pronounced. Although one knew it had to have been, it seemed more rehearsed than coached, and it seemed absolutely genuine.

Bendelladj, in contrast, had initially given the authorities passwords to decrypt his hard drives, but even that negotiation was described as "dicey". Bendelladj was described as extremely uncooperative. He did not accept any plea deal, and he is expected to appeal his sentence rather than cooperate with authorities in efforts to reduce time served.

Some the posts from the old "dark0de" cybercrime forum describing him as arrogant, reckless, and a braggart (those are the nicest terms) were entered into evidence, helping to paint an unflattering picture of his personality. His closing statement did nothing to counter that.

His apology and any assurances that he would never engage in such behavior again seemed perfunctory and hollow. At the end, it bolstered the prosecutor's closing argument that once he is free again, Bendelladj would go right back to cybercrime, except this time with the benefit of knowing how to remain untouchable.

Deterrence

The posts from the dark0de forum entered into evidence regarding both co-defendants spoke the loudest on the issue of deterrence. There was a time when SpyEye was outselling ZeuS, the king of all malware kits. In their time, both Panin and Bendelladj were praised for their talents and how they applied them, lauded for their successes, and viewed as heroes and role models among the members of one of the largest communities of the most dangerous cybercriminals on the planet.

The fact that many commented on the arrest of "bx1" (Bendelladj) showed that the cybercriminals were paying close attention to his fate.

Panin was seen as a prodigy. No evidence was presented that he actually stole anything, and many malware authors feel shielded from prosecution for what amounts to the manufacture of cyberweapons as long as that's their sole source of income.

In both instances, stiff sentences had extraordinary potential as deterrents. Of course, the degree of effectiveness of these types of deterrents, especially in cybercrime cases where perpetrators may enjoy a greater sense of impunity and isolation from victims, is a perennial debate. However, it's clear that the lack of a significant sentence would send an unequivocal message to those that might seek to fill the void left by the takedown of the SpyEye triad.

Outcome

Panin was sentenced first, after Bendelladj was removed from the courtroom. He was sentenced to 114 months (nine and a half years) followed by three years of supervised release. After his release, he will likely be deported back to Russia, in which case the stipulations of supervised release won't mater.

After a 30-minute break for another hearing, Bendelladj was returned to the courtroom and sentenced to 180 months (fifteen years). He also received three years of supervised release, but will likely be deported back to Algeria or Malaysia instead.

The consensus among the parties involved in the case is that the sentences were fair and sent the right message.

Damballa's Role

The US Department of Justice issued a public statement regarding the case and sentencing in which they thank Damballa for their assistance. That statement can be found here:

https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined

In efforts to protect others from this threat since its initial release, Damballa's Threat Research team has collected and analyzed vast amounts of data about the use of SpyEye in malware campaigns and reverse engineered new versions as they were made available by the author. We applied those findings tactically in protecting Damballa's customers, but also strategically in efforts aimed at eventual threat extermination.

Using this intelligence, Damballa's Threat Research team was able to help pinpoint the author of SpyEye and track the activities of top SpyEye operators throughout the cybercriminal underground, including the infamous "dark0de" malware and hacking forum taken down by law enforcement in July 2015.

Too often, threat disruption is less than permanent. Damballa's commitment extended well beyond the arrests of the SpyEye co-conspirators, and members of the Threat Research team continued to consult with law enforcement on technical arguments throughout the prosecution and eventual sentencing.

https://www.damballa.com/spyeye-sentencing/

About the Author

Don Jackson is a senior threat researcher at Damballa, the experts in network security monitoring for advanced threats. Jackson brings more than 25 years of experience in the information security sector to this role, where he is responsible for tracking threat actors engaged in cyber espionage, APTs, and nation state attacks, and enumerating their changing tactics, techniques, and procedures while tracking the actors network infrastructure.

Most recently, Jackson was the Director of Threat Intelligence for PhishLabs in their Research, Analysis and Intelligence Division. Before joining PhishLabs, Jackson was a Senior Security Researcher for the Counter Threat Unit at Dell Secure Works, where he executed advanced security research and development efforts and lead threat intelligence operations.

Jackson holds his CISSP (Certified Information Systems Security Professional) certification, and is a vetted and cleared member of the FBI InfraGard program (a partnership with private industry to protect critical national infrastructure), the U.S. Secret Service Electronic Crimes Task Force (ECTF), and the Georgia Internet Crimes Against Children (ICAC) Task Force. Additionally, he has been trained and certified by the Georgia Bureau of Investigation as a Children's Cyber Safety presenter and is a State of Georgia P.O.S.T. certified law enforcement officer.

BUSINESS REPORTER
DISTRIBUTED WITH
The Sunday Telegraph The Daily Telegraph

DATA SECURITY IN THE CLOUD

2016

Data Security in the Cloud will address the **practical aspects of securing data** in the cloud environment. The programme looks at how to **get the right services** to suit each company's requirements, **managing data classification and encryption**, and **improving access security**.

50% off

Reserve your place now online at **www.dsitc.co.uk**, or contact Tracey Meaneaux on **020 8349 6475** or **Tracey.M@business-reporter.co.uk**, quoting promo code **MP50**

PROVIDING THE STRATEGIES FOR SECURE CLOUD MIGRATION

WWW.DSITC.CO.UK

15 JUNE 2016 • LONDON

How to create a phishing attack prevention training?

The phishing attacks are getting more and more sophisticated and it's quite challenging to develop a training which would be a good prevention to such an occurrence. Through this article, we intend to provide some overview how phishing attacks happen, why they may cost the economy a lot and which strategies to their prevention could be.

Before we pass through all of these, we should try to clarify what *the phishing* is and how it works in a practice. For instance, during the previous time – you could easily get an email, social media post or any other communication message offering you a link to some amazing webpage.

So commonly, that web link would lead you somewhere or nowhere or you would immediately get a notification from your *anti-malware software* that clicking on that web destination – you simply downloaded some virus.

Anyway, whichever option of these three practical scenarios occurred, you would get a trouble because you would leave your IP address details to that website. How's that possible?

First, every owner of the website would deal with his *Content Management System (CMS)* being in position to confirm every *IP address* that would call his *website* from some *browser*. It's getting clear how non-difficult may be to use such information to conduct some skillfully coordinated hacking attack.

Once having an IP address of a computer within some

organization, you may so easily break into the entire network and not only run some attack which may get so obvious, but rather so silently steal *many confidential information* and using such a way of campaign do the bigger harm to that institution.

Those scenarios are happening so often in a practice and employers would frequently seek that its staffs should know how to cope with such a situation. Non-rarely, the big companies would invest in their employee's training looking for the best possible advices how to avoid becoming the victim of phishing campaigns.

As it's well-known, the phishing campaigns may go through the web, e-mails, social media or communication messengers and it's all about a link with *the uploaded malicious content* or such a nice web content that would just grab your IP address and make it available to some hacker's group or individual.

Further, we would hear many explanations how to recognize such a link, but times change and offenders are getting so *advanced* in their tactics to overplay us.

For instance, your bank may get a lovely message claiming that is some useful financial magazine offering you its blog's content for free. The banking staff may so unintentionally click on that link expecting to see *some financial news* which he would non-doubly get – because someone skillful would maintain that webpage.

At that stage, it would appear that nothing special happened at all – but very soon everyone would know that *so many confidential data* leaked out. Also, those phishing links could get packed as *shorten links* using bit.ly, ow.ly, buff.ly and many other standards.

Although the phishing would rise to a global concern, we would recommend to the companies supported by a *defense community* to build on the entire lists of advisable websites and social media accounts that may get trusted and used in a practice. The criterion to such a list creation would be strictly empirical. Maybe, some solutions in the future would automatize that process using *well-trained neural network-based software*.

About The Author

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

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

Cybersecurity Offers New Career Path for Veterans

By Sarah Brown

Veterans looking for the next step on their career path may find the perfect job match in the field of cybersecurity. With or without cybersecurity experience, nearly all veterans have skills that meet the basic requirements of the booming cybersecurity industry — and new programs are going after those skills to help fill thousands of open positions nationwide.

Explosive Growth in the Cybersecurity Industry

Cybersecurity, a relatively new field, deals with information protection in the virtual realm. It is also behind operating system and other updates for software and mobile devices.

Cybersecurity threats are growing and cybersecurity professionals create fixes to keep data for both companies and individuals safe.

According to Burning Glass Technologies, a Boston firm that develops technology to help match people with jobs, cybersecurity jobs are growing three times faster than other IT jobs. In 2014, there were more than 238,000 jobs posted in cybersecurity, accounting for 11 percent of all IT openings.

The Peninsula Press at Stanford University conducted a more recent analysis of cybersecurity job listings and found over 200,000 jobs left unfilled as of March 2015.

This trend shows no signs of slowing down. “The demand for the [cybersecurity] workforce is expected to rise to six million (globally) by 2019, with a projected shortfall of 1.5 million,” according to estimates by Symantec, a leader in software security.

Driving the demand is the increased incidence of major security breaches and evolving technology.

Cyber-attacks like the Ashley Madison hack, which exposed usernames, passwords, email addresses, credit card and PayPal account information, and details of more than 9.6 million transactions, have created a new urgency around information security.

With so much at stake, it’s no wonder that demand for cybersecurity personnel is high. It also makes sense that companies are looking to capitalize on the skills and training of former military servicemen and women.

Veteran Skillsets Meet Cybersecurity Needs

Information security positions require a broad range of qualifications, including analytical skills, problem solving, and the ability to understand the enemy — all of which match the skillsets of former military personnel.

Job specialties in the cybersecurity field further fit veteran strengths, ranging from penetration testers, who assess network defenses, to Chief Information Officers (CIOs), who set policies for entire companies and manage all aspects of IT departments.

Veterans, regardless of any cybersecurity training, also bring strong skills in the areas of teamwork, data analysis, and threat response, creating the ideal candidate for a career in cybersecurity.

In addition to the well-matched skill requirements, "U.S. News and World Report" ranked "Information Security Analyst" as the fifth best technology job for 2015, and the 34th best job overall. It's also been estimated that cybersecurity positions pay nine percent more — around $6,500 annually — than other IT jobs.

With a median annual salary of $88,000 and strong marks for growth and opportunity, cybersecurity offers veterans a potential career path that is both exciting and financially rewarding.

Adjusting Position Requirements to Match Candidate Offerings

With so much good news, why are so many cybersecurity jobs left unfilled? Partly to blame is the industry's current requirements, which are a bit more demanding than many veterans' technical certifications can accommodate.

To make it easier for vets to apply for cybersecurity roles, finance and consulting company PricewaterhouseCoopers (PwC) has recently changed its cybersecurity job descriptions to exclude the requirement of a bachelor's degree.

The firm also acknowledges that the transition from military life to the corporate world can be daunting. To make the adjustment easier for military hires, each veteran employee is assigned a "battle buddy."

Battle buddies are other former military personnel who have already made the successful transition to corporate culture. They help acclimate new veteran hires and check in with them throughout their tenure to help ensure longevity and eliminate turnover.

New Veteran Cybersecurity Training Programs

Job requirements aren't the only things changing in the cybersecurity industry. PwC and Internet security firm Solutionary have also developed intensive training programs aimed specifically at military personnel. PricewaterhouseCoopers' program, referred to as a "boot camp," just accepted its first class of 41 veterans on February 1.

During the PwC training, students will receive hands-on instruction to meet the needs of the cybersecurity field. Classes will range from computer fundamentals to network vulnerability detection.

Solutionary will begin its next classes in Omaha and Pittsburgh this spring through the SANS CyberTalent VetSuccess Immersion Academy.

The program is six weeks and includes the opportunity to obtain up to three GIAC (Global Information Assurance Certification) certifications while exploring areas of security, operations, auditing, management, and software security tasks.

VetSuccess training is offered at no cost to qualified applicants. Veterans can apply via an online aptitude test and must agree to work for the company for at least two years after training. Deadlines for the first classes are March 14 for Omaha and April 29 for Pittsburgh.

An additional VetSuccess Immersion Academy is planned for later in the year in Orlando.

The growing number of cybersecurity jobs and the growing number of veterans embarking on life after the military could be a match made in heaven.

If Solutionary and PwC succeed in creating a qualified pipeline of talent to fill their cybersecurity needs, perhaps other companies will follow suit.

About the Author

Sarah Brown is a tech specialist with a love of all topics relating to the IoT. She writes about upcoming technologies and internet safety. Sarah believes that the through entertainment, technology and the written word, we can all stay connected to each other and create a safe environment out in the ether.

Co-organiser :

MDEC
Driving Transformation

BIGIT TECHNOLOGY MALAYSIA 2016

Anchor Event of the Big Data Week Asia 2016

19 - 20 September 2016 | KLCC Convention Centre, Malaysia

Join us and be a part of 3,000 highly targeted delegates and 1,500 trade visitors across various industry verticals and job specialisations.

Special rate just for **Cyber Defense Magazine** readers: Use the code "**BMY16CDM**" to sign up!

EVENT SPONSORS:

TITANIUM SPONSOR

FUSIONEX experience.excellence

PLATINUM SPONSOR

DELPHIX

GOLD SPONSORS

cloudera | Life Is On Schneider Electric

HRDF Claimable

HRDF MALAYSIA

enquiry@bigittechnology.com

+603 2261 4227

Follow us @ BIGIT Technology

Visit our website

Organised by BIGIT a brand of OLYGEN

#BIGITMY2016

Building a Secure DNS Architecture for NFV

By now it's been well established that Network Functions Virtualization (NFV) provides important benefits to service providers. Not only does it provide cost savings by reducing operational costs and truck rolls to deploy new hardware, but it also improves the speed with which new network services can be introduced. Along with that flexibility, however, there are important considerations for companies to keep in mind, particularly when moving Domain Name System (DNS) infrastructure to an NFV implementation.

Security is one area in which moving DNS architecture to NFV raises unique security considerations. With software managing more of the networking functionality than ever before, a rethink of traditional protection should accompany the change. Many operators are still running open source or commodity software to protect the virtualized environment, but that entails risks they may be unaware of. Here are a few concerns that highlight the need for an intelligent approach to security in NFV.

- Traditional firewalls and intrusion detection systems aren't designed for securing DNS , especially in the NFV environment. The same flexibility that allows software to provide a higher degree of flexibility and configuration than a traditional architecture also means that there are more ways to potentially misconfigure network functions. This opens new avenues for attack, even as other aspects of NFV improve protection, such as centralization visibility and VM-level security. Even where security isn't compromised, configuration issues can cause a cascading effect that impairs the network's overall functionality, giving the appearance of a security issue where in fact none exists.
- Attacks such as DNS-based distributed denial of service (DDoS) can quickly overwhelm network resources by generating too many resolution requests for the DNS system to handle, effectively shutting down the network by preventing legitimate requests from being resolved. Other attacks replace valid IP addresses with those directing the requestor to malicious websites or use tunneling to attack individual virtual machines, encrypting and stealing information through channels not normally analyzed by traditional security software.
- Virtual machines provide network operations with centralized control over resources and enable the rapid deployment of on-demand resources. But just as with physical hardware, VMs are susceptible to malware infection. Once a machine is infected and isn't rapidly quarantined, the infection can spread to other machines throughout the network and disrupt functionality from within. Monitoring the virtualized environment requires a different set of tools from traditional network security.

With DNS-related security issues requiring additional attention as carriers adopt NFV, they should ensure that their security environment meets these requirements.

- Security for NFV should be built into the DNS architecture instead of bolted on. A higher degree of integration through the use of a DNS-specific protection helps minimize gaps in coverage that may be left by add-on solutions and can easily be exploited by attackers.
- To minimize the impact of an attack as it happens and address it as quickly as possible, the virtualized network needs to be able to rapidly scale resources by spinning up new machines without the need for operator involvement. Automatically adding capacity while the attack is managed prevents service interruption. In return, this reduces lost revenue and productivity.
- With dangers such as zero day vulnerabilities, NFV-based security should have the capacity to detect previously unknown threats by continuously analyzing network behaviour, while also defending against established threats such as off-the-shelf attack toolkits designed for a specific kind of attack.
- A DNS security strategy for NFV should include internal as well as external analysis and resource tracking. While many threats such as DDoS attacks may be external, malware on existing VMs is just as dangerous. The virtualized infrastructure needs the ability to track virtual machines that are provisioned, analyze their IP addresses, and monitor all traffic to detect suspicious behaviour on virtual machines in real-time. Additionally, it should have the ability to quarantine VMs to prevent the infection from spreading.
- Because configuration issues lead to security and performance problems, security in the NFV environment should include network discovery and automation tools that determine what network functions are properly configured and identifies potential problems.

With each new generation of technology, network planning has had to work to manage the risks while gaining the rewards, and NFV is simply the next step in creating tomorrow's highly dynamic, automated networks. When service providers proactively address security during the implementation process rather than as an afterthought, the result is a flexible, transparent network that meets immediate and future needs while keeping valuable resources safe.

About the Author

Dilip Pillaipakkamnatt,

Vice President, Service Provider Business, Infoblox

THE COMMERCIAL UAV SHOW ASIA 2016

1 – 2 September 2016,
Suntec Convention Centre,
Singapore

DEMONSTRATING REAL WORLD APPLICATIONS OF UAV'S

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

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

FEATURED SPEAKERS

Claus Nehmzow,
Digital Innovation Organization,
BP, Singapore

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

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

TOP SPONSORS & EXHIBITORS

SPONSORS:

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

EXHIBITORS:

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

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

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

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

VS.

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

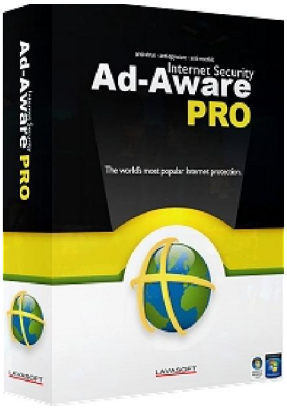
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting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

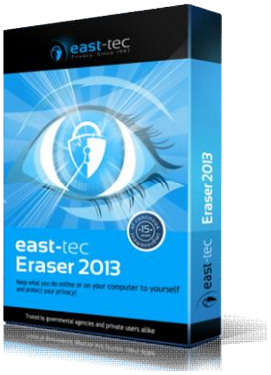
Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

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

SOURCES: CDM and NAISG.ORG

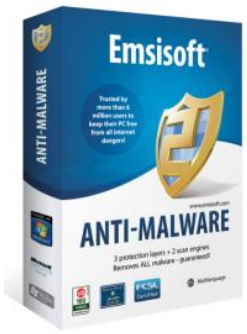




SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com

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



Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine May 2016

Sample Sponsors:

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

Cyber Warnings Newsflash for May 2016

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

ATM Skimming Malware Is Getting Scarier

http://gizmodo.com/malware-for-virtual-skimming-is-getting-scarier-1778067986

FBI Agent Testifies That The Agency's Tor-Exploiting Malware Isn't Actually Malware

https://www.techdirt.com/articles/20160522/16420734519/fbi-agent-testifies-that-agencys-tor-exploiting-malware-isnt-actually-malware.shtml

PERSISTENT EITEST MALWARE CAMPAIGN JUMPS FROM ANGLER TO NEUTRINO

https://threatpost.com/persistent-eitest-malware-campaign-jumps-from-angler-to-neutrino/118249/

Yikes! Adobe Flash bug is money-stealing malware

http://www.komando.com/happening-now/359919/yikes-adobe-flash-bug-is-money-stealing-malware

Mobile Malware: It's Not Your Apps, It's How You Use Them

http://www.wirelessweek.com/article/2016/05/mobile-malware-its-not-your-apps-its-how-you-use-them

Tech support scammers turn to screen locking malware to fleece victims

http://www.scmagazineuk.com/tech-support-scammers-turn-to-screen-locking-malware-to-fleece-victims/article/498110/

New And Improved Version Of Popular ATM Malware Spotted In The Wild

https://consumerist.com/2016/05/20/new-and-improved-version-of-popular-atm-malware-spotted-in-the-wild-again/

Furtim malware can run AND it can hide

http://www.scmagazine.com/furtim-malware-can-run-and-it-can-hide/article/497666/

How to keep USB thumb drive malware away from your PC

http://www.pcworld.com/article/3070048/security/how-to-keep-usb-thumb-drive-malware-away-from-your-pc.html

German nuclear plant's fuel rod system swarming with old malware

http://arstechnica.com/security/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/

Top Story: Massive malware attack - 1.5 billion smartphones at risk

http://www.komando.com/happening-now/358836/top-story-massive-malware-attack-1-5-billion-smartphones-at-risk

Cyber espionage malware discovered in Ukraine

http://www.itproportal.com/2016/05/20/cyber-espionage-malware-discovered-in-ukraine/

MALWARE-LACED PORN APPS BEHIND WAVE OF ANDROID LOCKSCREEN ATTACKS

https://threatpost.com/malware-laced-porn-apps-behind-wave-of-android-lockscreen-attacks/118099/

Why does old malware refuse to die? ...and is the IT security industry doing enough to kill it?

http://www.scmagazineuk.com/why-does-old-malware-refuse-to-die-and-is-the-it-security-industry-doing-enough-to-kill-it/article/497460/

People Are Willing To Risk Downloading Malware For "Diet Tips"

http://www.refinery29.com/2016/05/111106/malware-diet-tips-survey

Malware hunters: The battle to stop hackers targeting users with ransomware

http://www.abc.net.au/news/2016-05-18/malware-hunters:-the-battle-to-stop-hackers/7422752

Malware Museum Preserves Old Computer Viruses As Art

http://www.psfk.com/2016/05/malware-museum-preserves-old-computer-viruses-as-art.html

Malware Incident in MI Creates Potential PHI Data Breach

http://healthitsecurity.com/news/malware-incident-in-mi-creates-potential-phi-data-breach

Meet the malware that screwed a Bangladeshi bank out of $81m

http://www.theregister.co.uk/2016/04/25/bangladeshi_malware_screwed_swift/

Mozilla demands details on the FBI's malware hack

http://www.engadget.com/2016/05/12/mozilla-firefox-fbi-tor-malware-hack/

Mobile malware threat persists as attacks target iOS devices

http://www.itproportal.com/2016/05/19/mobile-malware-threat-persists-as-attacks-target-ios-devices/

Malware-as-a-service Is A Cheap Way To Spread Bitcoin Ransomware

http://bitcoinist.net/malware-as-a-service-is-a-cheap-way-to-spread-bitcoin-ransomware/

U.S. House bans Yahoo Mail, Google App Engine over malware concerns

http://www.computerworld.com/article/3069954/security/us-house-bans-yahoo-mail-google-app-engine-over-malware-concerns.html

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

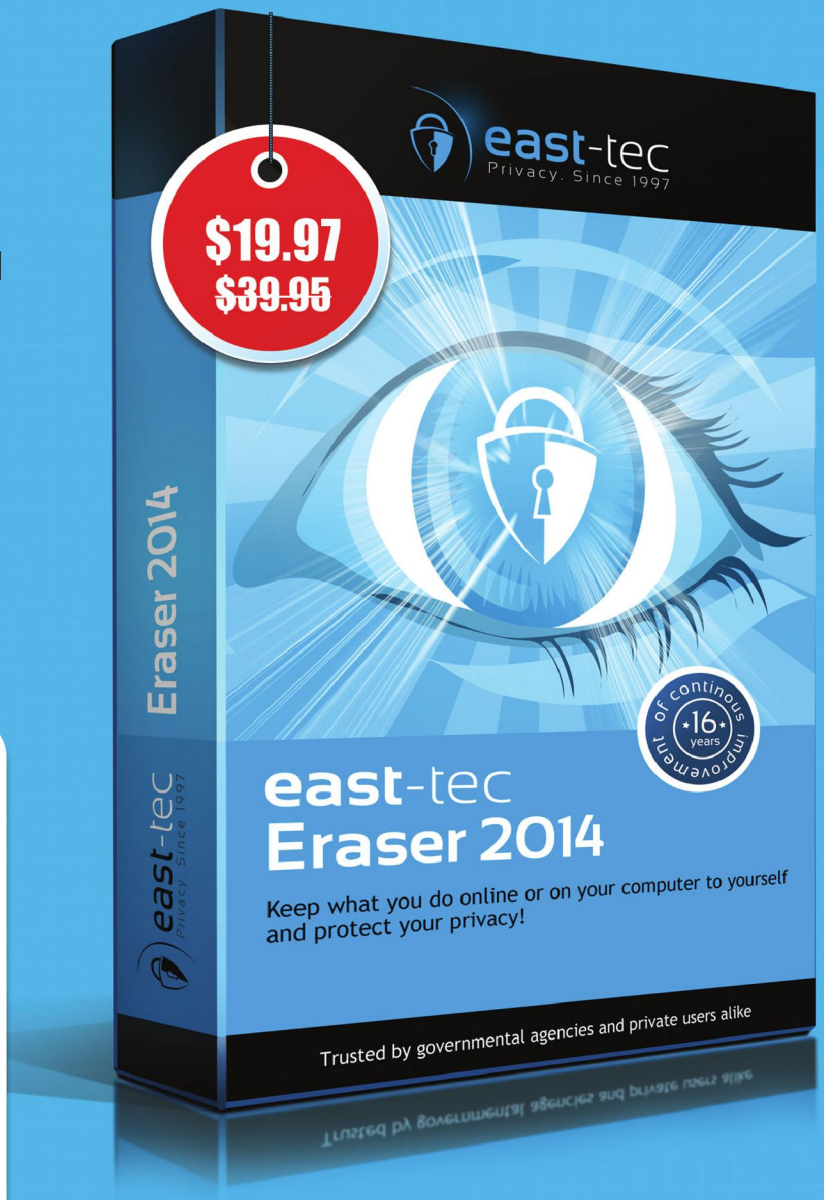
Cyber Defense Magazine - Cyber Warnings rev. date: 05/25/2016

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

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



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014

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