

CDM

CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IN THIS EDITION:

- ◆ **DDoS of Things**
- ◆ **Incident Response**
- ◆ **Ransomware Defense**
- ◆ **Password Security**

April 2017

MORE INSIDE!

CONTENTS

Cyber/InfoSec Unification: Time for a Change.....5

BSides Canberra – Australia’s Answer to DEF CON?14

The Dawn of the DDoS of Things (DoT)17

Part I: The Anatomy of a Wi-Fi Hacker in 201720

Simplifying Incident Response with Deception24

A gloomy vision of the future.....27

Cyber Security the Major Issue of 201729

This Data is mine, mine, mine, mine.....32

Austrian Hotel’s Ransomware Run-In Highlights IoT Vulnerabilities34

The best practices in dealing with ransomware36

Achieving Digital Trust in a World of Data40

New Attack with Seldom Used Vector44

INTEGRATION MAY ANSWER CHALLENGES IN MACHINE INTELLIGENCE.....46

CyberSecurity: Machine Learning + Artificial Intelligence = Actionable Intelligence.....50

Today’s Threat Landscape Requires Adaptive Security60

Shedding the Light on Deep Network Visibility for Cyber Intelligence Applications64

Office Depot70

Stop building higher fences and start searching the grounds72

Ransomware and the Internet of Things76

The Myth Behind Frequent Password Changes ...80

The Fatal Danger Lurking in Today’s Fortune 50084

CYBER WARNINGS

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

PRESIDENT

Stevin Miliefsky
stevin@cyberdefensemagaazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagaazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagaazine.com

KEY WRITERS AND CONTRIBUTORS

- Charles Parker, II
- Michael McKinnon
- Dr. Chase Cunningham
- Ryan Orsi
- Carolyn Crandall
- Kevin Coleman
- Angelica
- Jonathan Stock
- Alexandre Cagnoni
- Milica D. Djekic
- Drew Del Matto
- Martin Korec
- Smit Kadakia
- Dan Joe Barry
- Mike Seidler
- Scott Millis
- David Balaban
- Sarosh Petkar
- Tatu Ylonen
- Vineet Aggarwal
- Alisdair Faulkner
- Travis Rosiek
- Tim Green
- Sujain Thomas

Interested in writing for us:
writers@cyberdefensemagaazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Magazine: <http://www.cyberdefensemagaazine.com>

Copyright (C) 2017, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide. sales@cyberdefensemagaazine.com

Executive Producer:
Gary S. Miliefsky, CISSP®



The Why and How of GDPR (General Data Protection Regulation) for your business	87	National Information Security Group Offers FREE Techtips	111
E-Lenders: Hackers New Favorite Targets	97	Job Opportunities.....	112
Three Tips to Avoid Going Phishing	99	Free Monthly Cyber Warnings Via Email.....	112
Best Practices in Cyber Security for Businesses	101	Cyber Warnings Newsflash for April 2017.....	115
Tips to Help Boost the Security of Your MySQL Database	103		
The Electric Grid as Our Manager	105		
NSA Spying Concerns? Learn Counterintelligence	107		
Top Twenty INFOSEC Open Sources	110		

ATM & Cyber Security

rbr
EVENTS

 #ATMsec

London 10th-11th October 2017

The world's leading conference on physical and logical ATM security

Learn from case studies by the world's leading banks

Explore the latest technology solutions in expo area

Network with banks and industry experts



340+

Attendees



30+

Speakers



140+

Companies



40+

Countries

exhibit | sponsor | attend

www.rbrlondon.com/atmsec



NABSHOW
Where Content Comes to Life

NAB Show is proud to announce the NEW Cybersecurity Pavilion debuting April 22-27, 2017 at the annual event in Las Vegas.



In a 2016 survey of over 103,000 broadcast industry attendees, over **40%** were worried about breaches, ransomware and denial of service & want cybersecurity on the agenda.

This is a great opportunity to help educate and protect the Broadcast Media market from Cybercrime, Cyberterrorism, and DDoS attacks.

 **CONTACT US TODAY:** Grant Samples gsamples@nab.org 202-429-4184



KEYNOTE SPEAKER: Gary S. Miliefsky

Globally Recognized Breach Prevention Expert
"Offensive Cybersecurity for Broadcast Media"

PLATINUM MEDIA SPONSOR:

CDM

KEYNOTE SPONSOR:



PLATINUM INFOSEC SPONSOR:

DELLEMC

Cyber/InfoSec Unification: Time for a Change

Charles Parker, II

Cyber/InfoSec is relatively new in comparison to other scientific fields, e.g. physics, chemistry, circuit design, and others. Although InfoSec has been in existence well over a decade, this topic has been receiving a significant amount of attention in the last few years, due to the email provider breaches with instances of multiple compromises with single providers, utility company's equipment being compromised, utilities being shut down for limited periods of time, and fast food restaurants. The breaches and compromises have caused a mass amount of issues for all involved. This attentiveness has manifested its form with the increase in publications, articles, and even the president noting this is pertinent. As this is a newer discipline as related to others, this has not been through the intense, rigorous, and robust scrutiny placed on it that others have. This form of discipline would place a more mature framework on InfoSec. This is shown with other, more mature departments and areas of science such as physics, chemistry, and others.

InfoSec

The InfoSec field and community have held onto a different application of this, which has tended to be vastly unique in comparison to others. There may be a number of reasons, both known and unknown, leading the discipline to this end. This current state may simply be a function of InfoSec and its sub-fields not being as mature or seasoned as the others. There is a lack of a coherent standard across the InfoSec industry, which would provide guidance, structure, and ease of use for the pertinent, involved parties. Instead of implementing a simple set of standards applicable to each form of action, each sub-field continues to complicate the issue to our detriment with their own standards.

Autonomous Vehicles

Of areas of research and study within InfoSec, this is the most current and timely as the self-driving vehicles are predicted to be fully operational within the next five years. Ford, BMW, and other entities involved with this endeavor have clearly stated their goal is to have a fully autonomous vehicle operating by 2020-2021. With this goal set in place, the manufacturers and related entities are actively engaging their many architects and engineers to complete the task of engineering and manufacturing the fully autonomous vehicle. The companies involved with these project in various aspects including Google, Apple, Nvidia (Forrest, 2016), Tesla, Mobileye, Delphi (Reese, 2016), Ford (Reese, 2016; Raven, 2016), GM, and others.

Each may have their own idea of the architecture implementing communication protocols, and the other security and communication aspects that need to be addressed in order to be fully prepared. Each has their own budget, staff, and resources being applied to this long-term project. These entities may have wanted to work together at some junction, however this was not a viable option due to fear of losing their intellectual property (IP) or their lead in advanced technology in comparison to others.

This is also being researched by DARPA (Whalen, Cofer, and Gacek, 2017). One of the foci is to analyze the methodologies for securing the software located in the networked vehicles. This project would provide guidance, if followed, for the manufacturers and vendors. A framework for this involves utilizing The Update Framework (TUF) as a base and improved on this (Help Net Security, 2017). The new proposal is titled Uptane.

At this junction, the objective is open-ended. There is not a party at this point to lead the overarching project or the members with unified standards. If another business were to attempt to manage the campaign towards the autonomous vehicles without a nearly unanimous support, there may be only yet another protocol sitting with the others. There could also be a separate entity comprised of the vendors in the industry presently and academics. This would prove to be problematic. Several questions would be open for interpretation, including:

- a) Would this new entity carry the weight to adequately provide guidance and govern?
- b) Would each entity of the consortium have the same weight of input?
- c) Should this be based on the capital (money) contributed to fund this endeavor?

U.S. Department of Transportation (DOT)

Being researched concurrently is a push with vehicle-to-vehicle communication standards. The DOT is analyzing methods to reduce the number of vehicle crashes. With improved V2V communication, a significant portion of the vast number of vehicle crashes would be avoided and lives saved (NHTSA, 2016). The US DOT began this directed process of rulemaking in August 2014. This process focussed on the dedicated short-range communications (DSRC) for the inter-vehicle communications.

This has been studied for over ten years (US DOT, n.d.). The rulemaking has been manifested with the Preliminary Regulatory Impact Analysis (US DOT & NHTSA, 2016) proposing to establish the standard for the V2V communication. This will be proposed to mandate the standard to be used with the DSRC and other technologies that work directly with the DSRC. The phasing-in would begin, in theory, 2021 with 50% of the lightweight vehicles to have the DSRC capacity.

Internet of Things (IoT)

Within the InfoSec field, IoT is also a relatively new area. There are many manufacturers with their specialized products. There are Honeywell, Hitachi, Comcast, and T-Mobile (Meola, 2016), to list a limited portion of the established manufacturer. There are also a number of start-ups with Samsara, Notion, Losant, Helium, and others (Postscapes, n.d.). With the IoT products, InfoSec has been applied in various levels, ranging from none of all to a not significant amount. The IoT devices have been known to be notoriously insecure (O'Neill, 2016). As a method to secure the IoT, redundancy has been researched for a possible corrective action (Venkatakrisnan & Vouk, 2016).

A rather glaring recent example of the IoT insecurity has been the Mirai attack (Feingold, 2016). This bot army used IoT devices to attack its target (Leyden, 2016; Cimpanu, 2016; Heller,

2016). The victims of this include Deutsche Telekom (Kan, 2016), TalkTalk (Thomson Reuters, 2016), and Krebs on Security (Woolf, 2016; Krebs, 2016). These attacks and the bot army brought to light the lack of strict guidance and security to IoT. There has not been a rush to have security applied here. Over time this has been shown to be a higher priority project. The lack of a standard mandated to be applied has only further worsened the InfoSec environment. If there were to be a standard in place, the number and intensity of these DDoS would be substantially lower.

Bio-Medical Devices

These are medical devices implanted into or onto the human body and connected electrically. In this instance, the bio-medical equipment communicates to another unit certain data. The connected devices have a rather direct and overt impact on human life.

Security has been likewise applied to these devices, as with the IoT, in a rather haphazard manner. This is a clear indication that security, a unified set of guidance and standards, and protocols have not been a primary focus here also. The lack of focus is evidenced by the number of proof of concept attacks on the medical devices recently that have been in the news. There are a number of devices that fit well within the definition. With the biomedical devices having such a vital role in sustaining human life and the liability in the case of an epic equipment failure, a prudent business and engineering staff should apply a specific security baseline or at least some form of a minimum standard. This lack of a standard that has to be complied with shows yet another detriment to society and consumers.

Two recent examples are the pacemaker and diabetic pump. The pacemaker has been shown to have communication security issues, initially denied however later accepted by the manufacturer and FDA. There also has been like attacks on diabetic devices focussing on the communication vector.

Previously Attempted

Although this is a relative new sub-field of IT, there have been attempts to implement a security framework in the individual disciplines. Although the attempt has been made to implement these to strengthen the security to at a minimum baseline level, this governance has failed to effectively govern the relevant parties, and assist these parties to understand and comprehend the pertinence of these across the respective discipline. There may be varying levels of implementation, however on average the respective parties within each discipline have not embraced this.

IoT

With IoT, there has been no governing entity to direct research and which standards should be followed and applied. The US Department of Homeland Security (DHS). In order to work towards supplementing this and having a forum of principles to interpret, the DHS released a set of principles to secure the IoT devices (DHS, 2016; Schumann & Lieberman, 2016). This would not have been required if a mandated standard had been completed but is only a set of principles. As these are only designed to be a set of principles, these would not have to be

followed. There would be no impetus to apply these. This is still evident as the IoT devices continue to be compromised and used in attacks against others.

Biomedical

This area is vital as these pieces of equipment keeps people alive. A malfunction or hack of these may have dire consequences. To secure these, providing a solid, robust security framework would be prudent. Establishing this standard for security is not a new or novel idea. Klonoff and Kleidermacher (2016) researched diabetes and securing the connected devices to measure the user's glucose level. These devices monitor blood glucose on a static and continues level, insulin pumps, and the closed-loop artificial pancreas systems.

The researchers noted the Diabetes Technology Society (DTS) created in July 2015 the DTS Cybersecurity for Connected Diabetes Devices project. This standard was intended to be used with the industry, clinicians, patients, and others to gauge the applied cybersecurity. This is merely guidance, along with the FDA's guidance.

The FDA has put in place a set of rules regarding methods equipment manufacturers should manage their product's security (BBC, 2016). This was not a regulation, but a recommendation or suggestion (Hatmaker, 2016; Smith, 2016; FDA, 2016). The enforcement value of this would not be significant.

As these are multiple sources of guidance, the waters are still muddied at best. There is a bright point of light with this. There is another push for a protocol focussed on the "federated networking and computational paradigm for the Internet of Things..." (Madanapalli, 2017). This project to form the ROOF computing standard is sponsored by IEEE and is labelled as P1931.1.

Global Influence

In an attempt to implement a global standard, an international agreement for InfoSec with 41 countries was buoyed through the participants. This was known as the Wassenaar Arrangement (Camarda, 2016). This was not implemented.

Statutes

On the US state level, several states have recognized there needs to be statutes enacted regarding the security. Specifically, states have focussed on legislating the autonomous vehicles. The individual, respective states have enacted the legislation (NCSL, 2016). California, Florida, Louisiana, and Michigan have several statutes with two (2012 and 2016), four (two in 2012 and 2016), one (2016), and six (two in 2013, and four in 2016). The U.S. states have also introduced legislation regarding autonomous vehicles (NCSL, 2016) with 16 bills in 2015, 12 in 2014, and over 9 in 2013.

This, granted, is a momentous initial and continuing system towards securing the autonomous vehicles. Even with this tremendous amount of effect, the same issues abounds. These statutes and bills are per state. These are not unified. State "A" and state "B" may have statutes that are

similar yet different. The court's interpretation may also be different. Although this does appear to be a positive step, this is still indicative of a fractured set of direct guidance.

Commonality

The bi-product and symptom of this issue is rather clear. This has been manifested with the breaches in email providers (e.g. Yahoo twice), the federal government (e.g. IRS, FDIC, OPM, etc.), and too many other entities in the U.S. and abroad. The users personal data, intellectual property, and other data and information stolen during these breaches has been sold in the Dark Web, used for fraudulent activities and scams, and other deviant activities. This, among other factors, has led to a decline in the confidence associated with cybersecurity (Help Net Security, 2016). This is not only in the U.S., but on a global basis.

These endeavors have the same focus and goal of making the world a better place to live in via implementing a standard which everyone follows. This would take the form in the future as a reduction in the number of breaches, consumers being able to meander on the internet without fear of ransomware or being a victim of personal identification theft, industry not having to fear other nation states breaching their system for data and intellectual property.

The primary source of these issues continues to be the splintered InfoSec community standards and a lack of applied security. The community is working towards the same goals however on an individual basis. This, for example, would be securing the enterprise, securing communication between endpoints or intr-company, securing the data at rest, and other projects or transactions. This has not been focussed though. These efforts are not being accumulated at a sufficient pace. The advances with these are being artificially depressed by the infrastructure the community has self-imposed with each group being siloed. The effort may be much further advanced if these groups had been working together towards a single standard.

The space program is an example. Space exploration would not be at this stage if multiple groups in the 1950's and 1960's had been working on this. With this endeavor being under a single, driving force (NASA), significant advances were made.

Common Processes

There is a commonality with the processes being reviewed. Within each protocol, there may also be slight differences. With Wi Fi, there is the same action being undertaken. "A" is communicating with "B". These endpoints send and receive data and information. The data may consist of appointments, Human Resource Payroll records, new circuit designs, or other intellectual property. This process is replicated with a vehicle communicating with an application on a smartphone to unlock or start the vehicle, a person working on a laptop connecting to their work email, and biomedical equipment sending and receiving data.

These all have in common the act of communication of sensitive data. The security with this should be standardized with the same protocol, since this is the same act. The "A" and "B" parties are not necessarily pertinent in that these could be any business. The method or channel is however the pertinent factor.

Rationale

This conundrum has evaded a solution and governed direction. There are three primary options with this. As an indicator, the leadership can do nothing. This would only continue to perpetuate the InfoSec issues that abound in the news with breaches, compromises, data being stolen, and increased expenses for the affected parties due to incident response, credit monitoring, and lawsuits. This is optional.

A second option would be for the industry to regulate itself, apply common sense, and a sufficient level of resources to research, analyze, and implement these security rules. Over the years, this likewise has not been successful. This lack of focus, multiple protocols, and mixed levels of implementation have led directly to the breaches and compromised systems. This option likewise is not viable in the long-term. As an industry and field, the self-regulation in any form has been lacking.

The third option is to form an entity to research, publish, mandate, and evangelize these standards. The intent is not to overreach and be dictatorial, but to form a safer, more secure environment the industry has not been able to do so yet. The intent is also to be an altruistic movement. This would greatly assist the field, and users. The guidance to this point has been splintered. The standards in place effectually have been merely recommendations, with the exception of the state statutes for autonomous vehicles. These though are different per state with each state's judicial interpretation being unique. These specific industries (e.g. FDA, DTS, and DH) have their own guideline in place, which are not unified.

There should be a central standard for each type of transaction in InfoSec. For instance with communication, this should be secured with a form of encryption, regardless if this involves a vehicle communicating to an application on a smartphone, a user checking their email account from a phone, a website being secured (HTTPS) versus not (HTTP), SSO using SAML 2.0, or a pacemaker transmitting data to its base equipment and not in clear text or a low, inappropriate level of encryption (e.g. MD5 or AES 56). The data at rest also is notable, and should be encrypted with an acceptable protocol. Instead of each type of equipment or action having its own method, they should each have the same standard.

This is being proposed simply for the common good. These and other protocols being placed onto systems would be in the least a baseline needed to be secure. These standards being applied across the U.S. or further would provide a minimum baseline the industry and users would be required to follow. This would need to be on a national level due to the fluidity and dynamic nature of data and InfoSec. A user is able to scan an IP from nearly everywhere on the globe. A state border oriented system as it relates to InfoSec is meaningless.

Unification

Unfortunately, the number of attacks exploiting the same vulnerability continues to grow due to each industry's own standards guiding the same act, wasted concurrent efforts, and other factors. This has made it rather clear the industry is at a bit of a loss to govern itself in certain instances. There needs to be a single, unified application of InfoSec for each type of

transaction. This would not need to be overly rigid or unbending, but able to flex with each situation. No environment is the same, however the underlying needs and actions are the same.

The FDA has noted the industry is at a crossroads of InfoSec and technology (Schwartz, 2016). A unified InfoSec platform would be beneficial to the specific industry, the overall industry, consumers, and government with this single source of information and guidance to be applied. There needs to be an action to bring this altogether. This would ensure the relevant, germane parties are all operating under one set of rules and knows what to apply to comply. This, as a by-product, would also reduce the opportunity for ambiguity. With one set of standards being in place, deployed, and actively implemented, this would ensure the best practices are being reviewed and applied day-to-day, and not simply on an e-shelf collecting e-dust. As an example SHA-1 would not be implemented, while SHA-2 in one of its key size would be.

This would be used as a better means of applying security to each endpoint or transaction. The entities involved would clearly know the industry best practices as mandated by the appropriate standard. The parties would clearly know these would be required to be followed. There would be little doubt what security protocol and action to apply. For instance, legacy systems tend to use outdated security practices. This is due to several features including these simply being difficult to update, and the update being cost prohibitive. Although there may be hindrances to updating the system and security, it is still prudent to update the application. This may add value to the application and usage, however the costs may not be able to passed onto the clients.

The unified InfoSec protocols would remove the guesswork in this industry. The appropriate parties would know what standard and protocol to apply to your project. Everyone in the industry should be working the same set of standards. Any future changes to the protocol would be well-publicized and the germane audience would be notified as this would be well-known. This may be communicated with press-releases, email updates, tweets, and other accepted methods.

With a set of enforced standards as a simple baseline, issues with security would not continue to abound. Without this, the attacks will continue. These may become more frequent in occurrence and be larger. Future DDoS attacks may make the Krebs on Security DDoS appear to be a practice run.

Method

The process to arrive at these standards should not be arrived at lightly. There needs to be an abundance of caution and thought with this process. There would need to be a format for the process. This would be utilized to form and approve the standards. This removes the potential for ambiguity. With one format, all involved know what to expect. This would not be a government committee due the potential political skew, which would be counter-productive. As President Ronald Reagan is quoted, "The nine most terrifying words in the English language are: "I'm from the government and I'm here to help...".

These standards would need to be processed through a vetting process. This may be done with a committee composed of academia and industry members. This brings together the many

viewpoints. The process would provide for the best methods in theory and practice. These would be provided with a single person or faceless entity. With the group, there are many views and opinions. These are able to be molded together.

After the draft of the standard is put in writing, there should be testing and/or a pilot study. The standard would not be put into place without this being done in the various environments. This would also function to verify what works best across the industries.

Starting Points

This is a rather substantial project on several fronts. After gaining acceptance, which would not be a small feat in its own right, forming the committee would also require an immense amount of time, effort, and resources. As for the protocols, there are a number of generally accepted protocols for encryption, web applications, firewalls, authentication, defense in depth, Wi Fi, and log management. These would provide a starting point to be followed. The committee may begin to grow in depth the knowledge on these topics prior to reviewing future movements.

Mandated

There needs to be a form of motivation to adhere to these. Without the industry following these unified standards, these standards would only be yet another one in the field for review. In effect the community would be splintered yet further. The new set of standards would require some form of liability, as a motivator. If these standards are not followed, the entity electing not to follow it may be considered acting in a grossly negligent manner. These standards would be designed to be the minimum, baseline standard to be applied. These would also be based on industry uses, academia, and persons leading the thoughts in the industry.

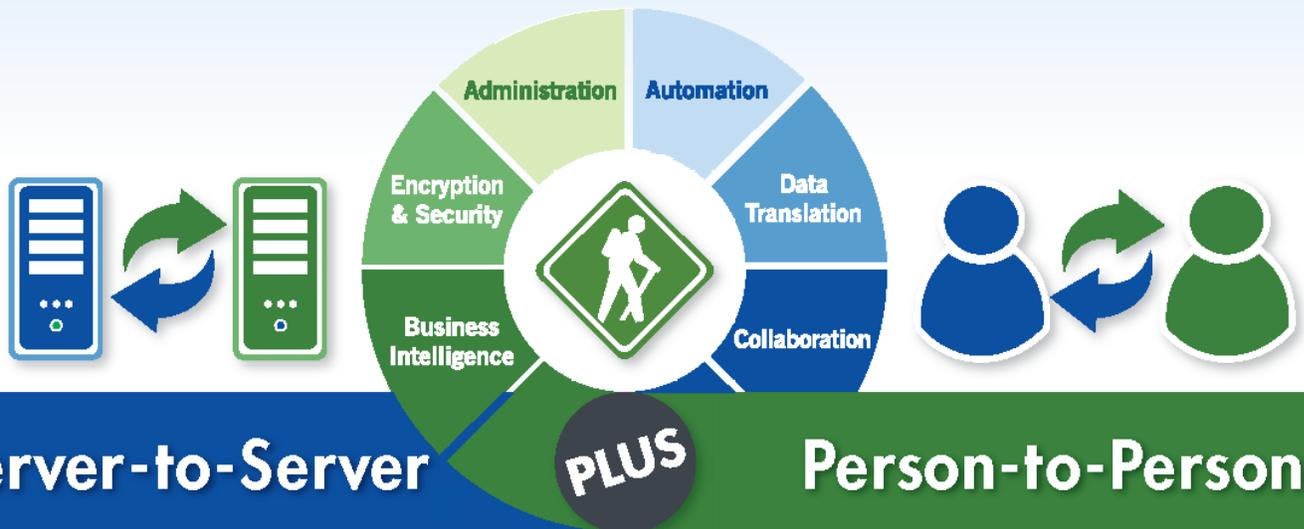
Summary

There has been a vast abundance of breaches and compromises in the different fields in recent years. There has been a leading indicator of potentially becoming a target-there is something the attacker wants to steal or keep people from accessing. The commonality with a majority of these attacks has been the attacker exploiting vulnerabilities. The vulnerabilities may have been remediated, however were not. With these standards being followed, there would be fewer breaches.

The effect of this would be resources not being wasted, a lesser degree of consumer and business frustration, and a safer world. Until this point, a set of standards to be used throughout the industry to this end has not been created or followed. With these in place, the industry would clearly know what standard is the best practice, and apply it to the project.

Without this being used, there will continue to be more compromises, breaches, and lack of confidence in InfoSec.

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™

GoAnywhere.com 800.949.4696

a managed file transfer solution by



BSides Canberra – Australia’s Answer to DEF CON?

A wrap-up of a recent hacking conference in Australia’s Capital City, Canberra.

By Michael McKinnon, Director - Commercial Services, [Sense of Security](#)

On Friday 17th and Saturday 18th March 2017, I had the pleasure of attending [BSides Canberra](#) once again. According to the organizers, this hacker conference is now officially Australia’s largest.

Juxtaposed by the City of Canberra, and the DEF CON like attendees – mostly male (although that’s improving) black-t-shirt-wearing hacker types (including me!) – this year was marked by a decidedly family-friendly environment with the most amazing community spirit you’ll find anywhere.



Spooks & Freedom Fighters

Let me set the scene and describe the contrast and surprising outcome you get when you put “spooks” and “freedom fighters” in the same room for two days.

Canberra is Australia’s capital city, located roughly half-way between Sydney and Melbourne and was established in the early 1900’s following this country’s Federation in 1901.

Accordingly, Canberra is home to a disproportionately high number of Government employees, and as such has a uniquely bureaucratic and dare I say, slightly boring feel to it. I imagine it might be like Washington, D.C. although I’ve never been there.

As you might expect in any capital city, there’s a large Military presence in Canberra, with a War Memorial and Museum, and it is home to the Department of Defence (yes, we spell it with a ‘c’) – including divisions like the [Australian Signals Directorate \(ASD\)](#) which contains Australia’s main defensive and offensive cyber capabilities.

You wouldn’t normally think of the ASD (akin to the NSA in this region) as being your typical hacker conference sponsor. Yet in Australia, the ASD are one of the biggest supporters of events like BSides Canberra. Perhaps it’s not that surprising given [they’re on a constant hiring spree](#) with a need to keep up with better-paying private sector employers competing for the same candidates.

Regardless, the irony of wearing a conference lanyard with “ASD” printed on it and a T-Shirt emblazoned with “DEPARTMENT OF DEFIANCE” shouldn’t be lost on anybody. It certainly wasn’t lost on [Australia’s Podcast-Love-Child-of-Infosec, Patrick Gray](#) in his keynote speech at the event.

Patrick remarked that we're lucky in Australia to be able to come together as individuals, as an industry, and with Government "spooks" to learn, discuss and shape the discourse of cyber security in a positive way. And he's spot on.

The main theme of [Patrick Gray's keynote](#) was a fascinating exploration of the motivations of whistleblowers. He provided an honest and refreshingly accurate assessment of figures like Edward Snowden and Chelsea Manning, amongst others.

The care and compassion that Patrick showed in the way he spoke about [Chelsea Manning](#), and how he explained her background and mistreatment was impressive. I spoke with several attendees afterwards and we all agreed we now have a deeper appreciation for what she was subjected to and an insight into the possible motivations for what she had done, thanks to Patrick.

Patrick's attendance at BSides was capped off by recognition of his significant contribution to the industry with a Lifetime Achievement award from the conference organizers – which he later quipped made him feel far too old.

BSides Canberra CTF - School Students Finding Zero-Days!

One of the features of any good hacker's conference is a Capture the Flag (CTF) competition, and this year the [BSides Canberra CTF](#) revealed some surprises.

The biggest surprise [that also made the news](#) was a group of local school students who discovered a zero-day vulnerability in the equipment being used to host the CTF challenge!

[Canberra Grammar's Code Cadets](#) led by teacher [Matthew Purcell](#) signed up for the BSides CTF and the team took out 4th position, which was quite the accomplishment for these young contestants.



It was so encouraging to witness first-hand the brilliant minds working in this young CTF team. Their accomplishments already prove that we're in very capable hands for up-coming generations.

Hardware Hacking, Lock picking and Workshops

BSides offered many other activities for attendees to roll their sleeves up and get involved in technical wizardry, starting with the delegate badge that required extra soldering to get it fully working – a deliberate ploy to get people interested in the hardware hacking village, and it worked.

In a separate workshop area, there was a constant stream of talks that covered everything from a Bug Bounty Simulation hosted by [Bugcrowd](#), to 3D printed Wifi Antenna making, and even lessons on how to build your own [SSH honeypot server](#).

The workshop area also included a lock picking village and tamper evident seal challenges. There was literally something for everyone, and certainly no excuse for not learning something new.

U.S. Cyber Security Industry Veterans win 3rd place in BSides Canberra CTF

Well-known industry veterans, [Chris Eagle](#) and [Aaron Hackworth](#) who were both visiting from the United States, teamed up to finish the CTF in third place – impressive when you consider they were competing against other teams that had an average of six or more people!

They called their team “Notsonoob” and indeed proved beyond any doubt they are, “Not” “so” “noob”.

Chris Eagle is a Senior Lecturer of Computer Science at the Naval Postgraduate School (NPS) in Monterey, California. He spoke at BSides Canberra about DARPA’s Cyber Grand Challenge of which he was chief architect.



Together Chris and Aaron accepted their oversized prize check with gratitude – and when I last spoke with them they were unsure exactly how they’d fit it on the plane home!

Bigger and better for 2018

The dates for next years’ BSides Canberra conference have been announced – 13th & 14th April 2018 – so if you’re planning a trip to Australia for a great hacker event, this is your chance!

About the Author



**Michael McKinnon, Director – Commercial Services
Sense of Security (<https://www.senseofsecurity.com.au>)**

Michael McKinnon is a cyber security expert at Sense of Security – a leading Australian cyber security consulting practice. With a core focus on achieving tangible cyber resilience for business and government, Michael is a trusted advisor to some of Australia’s best known brands and organizations.

He is a frequent media spokesperson and has been a member of the steering group committee for the Australian Government’s Stay Smart Online initiative. Michael can be reached online via email at michaelm@senseofsecurity.com.au and invites questions at any time on Twitter to [@bigmac](#).

The Dawn of the DDoS of Things (DoT)

Dr. Chase Cunningham, Director of Cyber Operations at A10 Networks

Last year saw an unprecedented uptick in the volume, size and scope of distributed denial of service (DDoS) attacks.

Led mostly by the [Mirai](#) malware, this drumfire of DDoS attacks took advantage of unsecured Internet of Things (IoT) devices to build massive botnets and launch mammoth DDoS attacks, the likes of which the industry had never seen. For the first time, DDoS attacks exceeded the 1 Tbps threshold.

And Mirai is still making waves.

In his keynote presentation at RSA Conference 2017, Intel Security Senior Vice President and General Manager Christopher Young warned that Mirai is thriving.

“We can’t think of the Mirai botnet in the past tense. It’s alive and well today, and recruiting new players,” he said.

Researchers suggested [Mirai was just the beginning](#). Making public the code needed to launch an IoT-powered botnet was a first salvo.

A rival botnet malware, [Leet](#), quickly followed on the heels of Mirai and used [SYN payloads different than Mirai](#). And in 2017, there’s sure to be another chapter in this saga.

Welcome to the DDoS of Things

This is the era of the DDoS of Things (DoT), where bad actors use IoT devices to build botnets which fuel colossal DDoS attacks. The DoT is reaching critical mass — recent attacks have leveraged hundreds of thousands of IoT devices to attack everything from large service providers and enterprises to gaming services, media and entertainment companies.

And it’s estimated that there will be [24 billion connected IoT devices by 2020](#).

As an attack method, it’s now even easier for attackers to commandeer IoT devices for nefarious purposes.

Many devices still use unsecure default credentials and are ripe for the picking.

Basic instructions are available online and the lucrative [DDoS-for-hire](#) market is expanding.

The DDoS of Things is powering bigger, smarter and more devastating multi-vector attacks than ever imagined.

This increased activity has lead Deloitte Global to predict that attacks reaching or exceeding 1 Tbps or more will be commonplace in 2017.

Deloitte posits that there will be an average of [one 1 Tbps attack or larger per month this year](#), as the total number of DDoS attacks surpasses 10 million globally.

Need more proof? This DDoS of Things infographic has numbers that are as startling as they are informative.

For example, there are roughly 3,700 DDoS attacks per day, and the cost to an organization can range anywhere from \$14,000 to \$2.35 million per incident.

And once a business is attacked, there's an 82 percent change they'll be attacked again.

Is your business prepared to battle the influx of IoT-driven DDoS attacks?

Don't Let the DDoS of Things Take You Down

DDoS attacks are damaging. Along with service disruption, they have a lasting impact that harms your brand, your revenue and your user experience.

You need to fight back and implement a comprehensive [DDoS protection solution](#) to defend your applications, services and brand.

A solution that can detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for your network infrastructure.

About the Author



A10 Networks Director of Cyber Operations Dr. Chase Cunningham (CPO USN Ret.) is an industry authority on advanced threat intelligence and cyberattack tactics.

He is regularly cited as a go-to cyber security expert and contributes to industry white papers, publications and speaking panels.

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

SECURITY & COUNTER TERROR EXPO



PROTECT | PREVENT | PREPARE

3-4 MAY 2017 OLYMPIA LONDON

Supported by



Home Office

The UK's Leading National Security Event

Understand and protect against the latest threats



350+
Leading exhibitors



100+
Free-to-attend conference sessions



3,000+
Products & services on display



50+
Live demonstrations



10,000+
Senior security professionals



Register free at www.sctx.co.uk/cyber

Follow us on @ACT_EXPO www.sctx.co.uk/linkedin

Co-located with



Sponsored by

Organised by

Part I: The Anatomy of a Wi-Fi Hacker in 2017

by Ryan Orsi, Director Product Management, WatchGuard Technologies

We all know the use of Wi-Fi is pervasive because people crave a constant digital connection. So much so, that they'll spend the day jumping from free public hotspot to free public hotspot. As a matter of fact, Wi-Fi now accounts for 60 percent of all connections to the Internet, according to Cisco's 2016 VNI report. The same report estimates there will be more than 540 million worldwide public Wi-Fi hotspots by 2021.

What people don't often think about, is that public Wi-Fi comes with a dark side – it's ripe for exploitation by hackers. That's right, hackers are hiding in the shadows waiting to spoof SSIDs and launch man-in-the-middle attacks in order to gain access to devices and steal sensitive information.

When we think about hacking, we tend to remember headline grabbing incidents, for example [Yahoo losing another billion user account identities](#), the [Ashley Madison hack](#), or [Russia tampering](#) with the U.S. Presidential Election. These attacks are generally considered layer 7 attacks, which are easier to see in the application layer. But, Wi-Fi hacking occurs much lower in the stack, down at layer 2, or the data link layer.

Since they're buried, they usually go unnoticed. (If you recall the [OSI model](#) is as follows: layer 1–physical, layer 2–data link, layer 3–network, layer 4–transport, layer 5–session, layer 6–presentation and layer 7–application.) But what's the anatomy of these layer 2 hacks?

The most commonly used Wi-Fi attack is a man-in-the-middle ([MiTM](#)) attack. A hacker spoofs a Service Set Identifier (SSID), and a landing page if one exists, and tricks a user into connecting to it, for example at a coffee shop. Though the victim may think they're logging into a secure page, they're actually handing email and password information directly to the MiTM that's perfectly mimicking the "Coffee Shop" splash page.

This is also known as an evil portal, and is just one of the ways a MiTM can extract sensitive information from a victim. All Wi-Fi hacks stem from someone (or something) becoming the MiTM.

Another type of Wi-Fi attack is called a Karma attack. Dating back to 2005, the Karma attack runs code on an attacker's access point (AP) and listens for beacon requests for connections like "Airline Wi-Fi" or "Coffee Shop." It then begins broadcasting that SSID into the air hoping a user associates with it.

Most devices automatically save past open SSIDs, so the next time the user is in range of the "Free Wi-Fi Coffee Shop" SSID, the device auto-connects without asking for permission. When Wi-Fi is left activated on a device, it sends out beacon frames into the environment looking to see if any saved SSIDs are in range.

A Karma attack reads these beacon frames and imitates the SSID a smart device is looking for, tricking it into connecting without requiring the user to press a button. Once that device is connected, attackers can monitor the traffic to and from the device, looking for sensitive information like passwords and credit card information, or direct the user to sites that load malware or even ransomware on the device.

(Pro tip: if you ever find that your phone is connecting an SSID from some past connection, for example you're in San Francisco, but it's connecting to one from a recent trip to Hong Kong, shut off your Wi-Fi, you could be in the presence of a hacker.)

Wi-Fi hacking with MiTM and Karma attacks historically has required serious domain knowledge and command line skills. But today, a YouTube search for "Wi-Fi hack" generates more than 2.8 million hits, with "how to" sitting atop the results. These tutorials can teach anyone with a spare weekend how to hack over Wi-Fi.

If searching YouTube wasn't easy enough, there are also tools like [Hack5's Wi-Fi Pineapple](#) that are freely available for purchase starting at \$99 USD. They include an intuitive GUI, how-to videos, and a third-party module marketplace for powerful hacking tools. The Wi-Fi Pineapple does the job that hardcore Wi-Fi hackers used to do manually and it makes MiTM'ing very simple. An attacker could have one in their backpack performing a Karma attack, listening for SSID beacon requests, adding those SSIDs to a list to broadcast through the AP radios and voila! Victims start to connect.

Recently at the RSA conference, I broadcasted fake SSIDs for public Wi-Fi (for research purposes only) to see how many attendees would carelessly connect. We had more than 2,400 connections. Had we been hackers, we could have wreaked significant havoc on the users. Instead, we directed them to a splash page with security best practices. (Read the entire blog post about this research [here](#).)

If a hacker really wants to get fancy, he/she could even break the connection between a legitimate AP broadcasting "Coffee Shop" and a client by spoofing the BSSID (the MAC address) of the AP. Then use the Pineapple to flood the client with IEEE deauthentication frames. This will tell the client that the AP no longer wants to play. The victim's device then rescans for "Coffee Shop," this time finding the Wi-Fi Pineapple ready and willing to accept the connection for a fake "Coffee Shop."

As you can see, Wi-Fi hacking doesn't have to be all that complicated, and easy-to-use graphical hacking tools are accessible to anyone willing to learn. Unfortunately, people are not even safe when browsing encrypted HTTPS websites. After MiTM'ing a victim, it's very possible to intercept credentials for bank websites, email, shopping and more.

New, easy-to-use tools have resurrected an old tactic from 2014 called SSL Stripping. It tricks web browsers into bypassing HSTS (HTTP Strict Transport Security) policy and sends information to the MiTM over plain text.

The reality is that credential interception happens every day across Wi-Fi networks around the world. It offers one of the highest rewards versus risk payouts for cybercriminals, and these “little” hacks could have huge implications on the threat landscape. Consider this: if a senior executive has his or her Gmail password intercepted while sipping a cappuccino and accessing email on public “café” Wi-Fi, it’s not likely he or she knows they’ve been hacked. But, this information could be used to gain access for a larger hack or breach. That’s why Wi-Fi hacking is so scary.

If these attacks are so prevalent, why isn’t the industry doing more to prevent them? First, the victims often don’t know they’ve been hacked. The public puts blind trust into these public networks, which is surprising considering users can get passed off from their carriers to a public network without knowing it.

Second, it’s really hard to trace these types of attacks due to the MiTM and the fact that it’s over a public network. And third, AP vendors haven’t traditionally had a good solution for the problem, so they’re not working to raise awareness.

If using public Wi-Fi exposes the public to a variety of security risks, and the MiTM attack is the root of most Wi-Fi evil, what’s the solution? VPNs (Virtual Private Networks) can make connecting safer, but not everyone knows how to use a VPN and it relies on the end-user taking action.

Passwords on SSIDs can also help, but the four-way WPA2 handshake is easily decrypted in minutes by GPU accelerators or other resources on the dark web.

What’s the answer?

In part two of this series titled “Defending Your Airspace,” I’ll explain how organizations can use the latest technology to provide secure public Wi-Fi, and take the end-user out of the “security equation.” In the meantime, be diligent when at the local mall or coffee shop.

About The Author

Ryan Orsi is Director of Product Management at WatchGuard, a global leader in network security, providing products and services to more than 75,000 customers worldwide. Ryan leads the Secure Wi-Fi solutions for WatchGuard. He has experience bringing disruptive wireless products to the WLAN, IoT, medical, and consumer wearable markets. As VP Business Development in the RF industry, he led sales and business development teams worldwide to success in direct and channel environments. He holds MBA and Electrical Engineering Degrees and is a named inventor on 19 patents and applications.

Ryan can be reached online at @RyanOrsi and at our company website www.watchguard.com/wifi

CYBER SECURITY SUMMIT 2017

The Cyber Security Summit connects C-Suite & Senior Executives responsible for protecting their companies' critical infrastructures with innovative solution providers and renowned information security experts.

CyberSummitUSA.com >



REGISTER AT CYBERSUMMITUSA.COM

50% OFF ADMISSION WITH PROMO CODE: **CDM2017**

STANDARD TICKET PRICE \$350

The Cyber Security Summit Expands into Key Markets in 2017

Dallas, TX
Friday, May 5, 2017
Omni Dallas Hotel

Seattle, WA
Thursday, June 1, 2017
The Westin Seattle

DC Metro
Thursday, June 29, 2017
Ritz-Carlton Tysons Corner

Chicago, IL
August 8

New York
September 15

Boston, MA
November 1

Los Angeles
November 29

Engage in Interactive Discussions & Roundtables Including:

- The Compliance Nightmare: Using Your Solution Provider as a GPS For Navigating The Perilous Road To Compliance -
- Hacking Back & Its Legal Repercussions. What's Your Strategic Incident Response Plan? -
- Emerging Risks Likely To Become Major Threats Facing IoT and Big Data? -
- Protecting Your Enterprise from Corporate Espionage: Keeping Insider Threats Outside -

The Growing List of 2017 Solution Providers Includes: (Partial List)



To Exhibit Contact Bradford Rand at [212.655.4505](tel:212.655.4505) ext 223 or BRand@CyberSummitUSA.com

Simplifying Incident Response with Deception

By Carolyn Crandall, CMO

Computer security incident response teams (CSIRTs) continue to struggle to deploy effective incident response. A combination of more data to sift through to detect malicious activity; limited time, manpower and expertise resources; and the more severe consequences of data breaches all contribute to the challenges of effective incident response.

Integrating deception into incident response solutions has caught the attention of industry experts. KPMG highlighted many of the common mistakes teams make in deploying, maintaining and enhancing incidence response solutions in a 2016 [report](#). In addition, in another 2016 report, ["Best Practices for Detecting and Mitigating Advanced Threats, 2016 Update."](#) Gartner analysts note, "When possible, consider your IR investigation and triage efforts with integration between forensic analysis tools and other security monitoring software to more rapidly respond to potential suspicious security events when they occur." They also noted as a best practice to consider, "Utilizing deceptions across endpoint, application, data, identity (fake credentials) and network infrastructure to enhance your advanced-threat and insider-threat detection goals."

A new generation of innovative technologies has emerged to address these challenges. At the forefront of these is deception. These new solutions accelerate incident response by not only providing early attack detection, but also by automatically taking disparate attack information, correlating and displaying it on one dashboard where the solution can score it based on the type of attack activity, and creating playbooks CSIRTs can use to create repeatable processes, simplifying future incident responses. New incident response solutions based on deception platforms integrate with third party prevention systems, such as firewalls, SIEMs, NAC, and endpoint (EDR) to automatically block and quarantine attacks. This expedites response actions, prevents the attack from continuing to spread through the network, and empowers threat hunting for forensic artifacts in other parts of the network to confirm they have eradicated the attack. To integrate and automate incident response using deception, CSIRTs should have an understanding of how these solutions work and key capabilities requirements.

Gaining a Complete Picture

Incident response solutions should be able to ingest information from threats detected by deception engagement servers, SIEMs and other devices, correlating attack data, logs, endpoint memory forensics, and use of deception credentials by tracking failed log-ins. This approach provides a more complete picture of the attack and ultimately reduces false positives and investigation time, thereby simplifying overall incident response.

Additional Attack Insight via Adaptive Deception

Solutions should apply advanced analytics to correlate the multi-source attack information and be able to open communications to Command and Control Centers (C2C) in order to understand the attacker's lateral movement and any polymorphic activity. With advanced

deception platforms, the solution will also be able to auto-deploy additional decoys to gain supplemental insight into attacker activities. This hinders attackers by causing them to spin meaningless cycles in a hall of mirrors or labyrinth of deception

Automate Incident Response Handling

The incident response solution should automatically share correlated attack information with prevention and detection systems and, based on the security team's policies and playbooks, accelerate the incident handling with automated blocking and isolation of an attack for quick handling and remediation.

Collaboration Enables a Better View

Creating a single source for the security team to review correlated attack information and to collaborate on incident response allows teams to see real threats and activity patterns that they might have missed or ignored based on a partial view of threat activity. In addition, it creates a consolidated environment for information security teams to post-incident response activities and comments, allowing for effortless coordination and sharing of data across the organization without losing valuable historical data.

Effective Remediation

Swift and effective incident response includes remediation, and the solution should include not only the quarantine of an infected system but also a transfer of information required to generate a trouble ticket with applications such as ServiceNow or Jira. Providing the IT Help Desk information on exactly what the team needs to promptly remediate an infected system or unit will drive faster resolution and, in many cases, the proof needed to take critical systems off-line for repair.

Deception Adds a New and Powerful Weapon to the CSIRT Arsenal

Incorporating deception capabilities into incident response is a powerful addition to the suite of solutions available to CSIRTs. Deception adds the visibility and efficient detection of in-network threats but also goes one step further in enhancing the value of current security infrastructure. Hand-in-hand, deception platforms, prevention, and SIEM systems can work together for efficient continuous threat management to build a stronger defense against today's sophisticated attacker.

About the Author



Carolyn has over 25 years of experience in high tech marketing and sales management. At Attivo Networks she is the Chief Marketing Officer responsible for overall marketing strategy, building company awareness, and creating customer demand through education programs and technology partnerships. She has built leading brand strategy and awareness, high-impact demand generation programs and strong partnerships for some of the

industry's fastest growing high-tech companies including Cisco Systems, Juniper Networks, Riverbed, Nimble Storage, and Maxta.



C5

Business Information in a Global Context

Cyber Defense Magazine is partnering this Conference
Get **15% off** by quoting **P15-999-CDM17**

23-24 May, 2017 | London

CYBER GOVERNANCE & STRATEGY RESPONSE

CRISIS MANAGEMENT IN THE WAKE OF A CYBER ATTACK

GAIN PRACTICAL CORPORATE INSIGHT FROM:

Simon Fisher
GRC Lead
TalkTalk

Richard Magnan
General Counsel
Rising Tide

Oisín Fouere
Managing Director
K2 Intelligence

Andrea Cremonino
Risk Management, Operational
& Reputational Risks
buddybank

Avi Weisman
VP

Ruby Corp.
(Parent company of **Ashley Madison**)

KEY TOPICS INCLUDE:

- » Good Governance
- » Preparedness
- » General Data Protection Regulation – What This Will Mean for a BREXITing Britain?
- » Incident Response & Putting Together an Incident Response Team
- » Role of Cyber Insurance
- » Crisis Management and Reputational Risk
- » Forensic Investigation and Gathering Evidence
- » Civil and Criminal Remedies and Effectiveness
- » Unique Jurisdictional Issues
- » Strategies for Prevention

New technological innovations are creating new criminal opportunities in which the computer and the World Wide Web are used as an instrument to pursue illegal actions. It is estimated that two thirds of big UK businesses have suffered a cyber-attack in the past year and it is now one of the most-reported types of economic crime.

With cyber attacks grabbing headlines around the world organisations are realising that they need to move from a reactive, fire-fighting mode, where cyber may be regarded as merely an IT issue, to a proactive stance so that boards stay ahead of and manage this potentially devastating risk.

GAIN IN SIGHT INTO CRISIS MANAGEMENT IN THE WAKE OF A CYBER ATTACK

A MUST-ATTEND EVENT FOR:

- ✓ Chief Information Officers
- ✓ Chief Information Security Officers
- ✓ Data Protection Officers
- ✓ Cyber Security Professionals
- ✓ Information Risk Managers
- ✓ In-House Counsel and Legal Directors
- ✓ Data Protection Lawyers
- ✓ Computer Forensics Experts and Forensic Accountants
- ✓ Cyber Insurance Providers

A gloomy vision of the future.

Kevin Coleman, Chief Strategist Independent Software, Inc.

In 2015 Symantec discovered more than 430 million new unique pieces of malware, up a whopping 36 percent from the year before. If you decompose that figure, on average that equates to slightly over 14 new strains each and every second. Can you imagine if your antivirus software had to examine every file on your computer for those 430 million signature files. Now think about all the time and updates that would be required to keep your antivirus up-to-date.

By all indications 2016 was another record year for the release of new strains of malware. It is no shock to find that Deltek's Federal Information Security Market Report suggests that federal agencies struggle to stay ahead of the cybersecurity threats. With figures like those just presented, who could blame them?

But wait there's more – much more! Gartner projected a total of 6.4 billion connected "Things"(Internet of Things) would be in use in 2016. As we are all aware, the vast majority of those IoT devices are unprotected and vulnerable to cyberattack.

In a 2016 cybersecurity report AT&T stated that there was “458 percent increase in the number of times hackers searched Internet of Things connections for vulnerabilities.”

Did your budget and resources increase at the same 458% pace as the hacker IoT scans? No! Did your budget and resources increase 36% like the malware did in 2015? No!

Consider this, a recently released report by Cybersecurity Ventures projected we are going to spend over \$1 trillion globally over the next five years. After all of that spending, they project the losses due to cyberattacks and cybercrime will exceed \$6 trillion.

One has to wonder if we did not increase spending like this report projects, what the losses would be!

To recap the current situation, we don't have the budget to keep pace with the ever increasing number of cyber threats. Even if we did, where would we get the resources necessary for this task.

One report states that it takes six month or longer to fill a cybersecurity vacancy. After all, they are in short supply globally and it does not appear college enrollment in this specialty is keeping up with demand.

Even if college enrollment and graduates were keeping pace, they have little or no practical hand-on experience that is so critical in cyber security and defense. Oh, we should also not forget that many of those in cybersecurity are entering retirement age, so this problem is likely to get much worse.

To keep pace with the rapidly changing cyber threat landscape, things must change! An event looms in the horizon that is likely to become the catalyst behind the change. The dirty little secret that no one talks about will likely be that catalyst.

When a cyberattack occurs and it results in the death or deaths of individuals and that information becomes public, the outcry and demand for change will become so substantial, the industry will have no choice.

There have been rumors and unsubstantiated and unconfirmed reports of this taking place periodically for years. Once confirmed, cybersecurity will become baked-in to every product that connects to the Internet that has a sensitive function or produces data that is relied upon for sensitive systems.

One has to wonder if charges of manslaughter will be brought against cybersecurity professionals and or system owner operators when such an occurrence takes place.

The Law Dictionary defines manslaughter as the “unlawful killing of a human creature without malice, either express or implied, and without any mixture of deliberation whatever; which may be voluntary, upon a sudden heat of passion, or involuntary, in the commission of an unlawful act, or a lawful act without due caution and circumspection.”

Or perhaps this will drive the creation of a new term specifically created for cybersecurity lapses that result in the death or deaths of individuals. Even if that does not occur, we have the civil proceeding that is becoming a much more common occurrence when it comes to cyber events.

We must not forget, if it does occur, there is little doubt that the government will get their share of the blame as well. All in all, a gloomy vision of what is likely to come.

About the Author



Kevin Coleman is a seasoned technology professional with a comprehensive background in emerging technology strategy and cyber security. He is a recognized subject matter expert on the issues and opportunities created by technology.

His work in cyber includes speaking at the United Nations, before members of Congress, at U.S. Strategic Command and lecturing at the Army War College, Air Force Institute of Technology and the Navy postgraduate program.

He is also well known for his keynotes for corporate events and webinars.

Cyber Security the Major Issue of 2017

Technology has provided services to the whole humanity like no time ever before. Now in this contemporary world, everything is connected such as cars, cities, planes, homes and even the animals. The technology in the shape of software is everywhere. So, everything is changing such as how we talk, how we behave and how we interact with the environment. Now in the contemporary world technology is integrated with the human's DNA. We are becoming fully dependent on the technology. In-case technology in the shape of security fails in a certain way, and then it makes us vulnerable. Sometimes it happens when our phone runs out of battery and we feel very odd because you have the lack of access to GPS, contacts and many other purposes. Now you can understand how much technology has its influence on our lives.

In the modern world, we all are protected by technology tools; if not then we will pay a heavy cost and suffer from horrible consequences in routine life.

Cyber threats do not remain limited:

There is no doubt about that, technology is serving us enormously, but I have serious concerns about our up -coming future. Therefore, we have to look forward sincerely about the issue of cyber security which is currently affecting technology. Cyber security is the major issue of the current year, and technology is continuously suffering and becoming insecure. Things are not getting better and [cyber security issues are at their peak](#) presently, what will happen in near future. We are meeting with daily basis issues such as hacking, pacemakers have been hacked, plan system has hacked and recently all the IOS and Android devices have been hacked by the US intelligence agency in the United States of America. The banking software has been hacked and billions of dollars theft because of cyber- attacks. I have just highlighted few of examples by doing a bit research work, in reality, infinite cases of cyber security issues are identified in technology, the victim firms had highly best security systems. Even then, plenty of cases have occurred every single year.

Cyber Threats are Progressing:

The cyber threat environment is progressing dramatically, according to the Fire Eye Marsh& McLennan Cyber Risk report. The concerns are regarding breaching the financial and personal data along with the specter of even larger and devastating threat. The Cyber-attacks are possible in Europe's critical infrastructure such as power stations, aviation systems, transportation networking, water system programs and nuclear facilities. Cyber- attacks are progressing rapidly in current year especially, according to some new reports.

Another report found that [cyber-attacks have been growing quickly](#) over the last couple of years, and there's nothing to indicate they won't just keep increasing. If these attacks happen at the same pace then the indication of attacks might be impossible and the attacks will be easier and dangerous. The main factors behind the cyber-attacks such as lack of knowledge and necessity of cyber security and some companies have awareness and know the importance, but don't know how to make the effective security systems to prevent cyber- attacks.



Threats Actors are everywhere:

We often have to think sometime who are people who gain advantages cyber-attacks issues? Who used them? All the people who perform illegal agendas by doing cyber-attacks are commonly known as "THREAT Actors". They usually breach the sensitive information and sell it for the sake of money. The hacker's community is one of the main focuses who are well-trained professionals who work in companies and improve security systems, they fully aware of lope holes existed in any company's security system. So any dishonest hackers may do cyber- attacks on any particular company's security system. There is also a community which is known as hacktivists, they

are socially motivated under any unknown organization. The cyber terrorists are not common like others, but in future due to the lapses in security systems could become familiar to the general public. Cyber-attacks can be launched by any enemy state against their rival or enemy country. So attacks can be possible through any particular individual groups, government and from any cyber terrorist group.

Economical- Effects of cyber security breached:

Cybersecurity problems can occur anywhere, this type of attacks caused billions of dollars losses until the security system not be made fully secure and efficient. There are some examples such as smart alarm simple safe hack and affected almost 300000 electronic devices and fixing was possible I case of replacing all the devices. UK based company named as Talk Talk was attacked and almost lost 50 million Euros. So, we can claims that the cyber security issues are progressing every day along with possible deadly impacts on the economy. So these attacks are directly hitting us, because of our full dependence on technology. There is a still plenty of time to stop all kinds of cyber-attacks and we should work together to control the attacks before it will too late.

About the Author



[Angelica](#) is a social media expert, digital parenting and developer at [Danger for teen](#). He is love write to technology and relationship issues and their solutions. To know more about him follow twitter [@angelicadowson2](#)



INDUSTRIAL CONTROL SYSTEMS

ICS Smart City

15-16
May 2017
Intercontinental
Hotel The City,
Doha, Qatar



PREVENT, PROTECT, DETECT, MONITOR AND RESPOND TO THREATS WITH CYBER SECURITY SOLUTIONS FOR SMART CITIES AND CRITICAL INFRASTRUCTURE IN QATAR

KEY SPEAKERS INCLUDE:



Samir Pawaskar
Manager – CyberSecurity Strategy and Policy, Cyber Security Division, **Ministry of Information & Communications Technology (QATAR)**



Oriane Barat
Legal Consultant Minister's Office, **Ministry of Transport and Communications**



Pascal Dutru
Legal Unit Manager, Qatar Communications Regulatory Authority, **ictQATAR (QATAR)**



Dr Amy Hochadel
Global Cities Lead, **Future Cities Catapult**

TOPICS TO BE DISCUSSED

AT INDUSTRIAL CONTROL SYSTEMS SMART CITY QATAR FORUM INCLUDE:

- Assessing developments in policies and strategy to protect critical infrastructure
- Qatari sector case studies – Banking and Utilities
- Risk management strategies, Doha "Smart City" experience
- Industrial Control Systems (ICS) – legacy systems, incident response and mitigation measures
- Integrating Industrial Control Systems to fast-track development
- Developing a regulatory framework which provides the necessary safeguards
- Qatari sector based case studies – Hydrocarbons and manufacturing
- Practical issues address – People training, top threats discussed

**SPECIAL OFFER FOR
CYBER DEFENSE MAGAZINE
SUBSCRIBERS,**
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

QUOTE **ICSM17** AND GET
A 10% DISCOUNT ON THE DELEGATE FEES

**Secure your place now!
To SPONSOR or ATTEND**

send an e-mail to
Jessica.bousamra@acm-events.com

SILVER SPONSOR

SIEMENS

ASSOCIATE SPONSOR

 **DARKTRACE**

MEDIA PARTNER

CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

ORGANISED BY:

 **acm**

www.icssmartcity.com

Advanced Conferences and Meetings FZ-LLC
T: +971 4 563 1555 | F: +971 4 422 7548 | E: opportunities@acm-events.com

This Data is mine, mine, mine, mine.

by Jonathan Stock, Cyber Security Recruitment Consultant, IntaPeople.

It seems every time I write an article I could mention Trumps' approach to cybersecurity; watching him is like an old Animaniacs show with Yakko, Wakko and Dot causing mayhem throughout the White House.

Instead let's focus on the positives of the past week; Tom Brady became the most loved quarterback in the world, Beyoncé announced (in an odd, yet typical celebrity fashion) she's got a new brood en route, and the Queen is the first monarch to reach a Sapphire Jubilee - hats off to you ma'am!

Last week we had Data Privacy Day, a day to raise awareness and to promote data protection best practices.

Much like Cyber Security Awareness Month (October if you are wondering) it's a chance to educate the masses, to make sure that people outside of the security industry are aware of the pitfalls of data privacy and how important it is to keep data hidden, tucked up and warm like a Mogwai on a rainy day!

Now there are various quick fixes which can allow you to keep your data safe from the hackers of the world. They are not tricky, they are not technical, just nice and easy tips to help you keep everything as hidden as possible.

Let's take for example public Wi-Fi; it's brilliant isn't it? You can stream content whilst your partner shops for the 100th pair of shoes on a Saturday afternoon, but it's not the most secure network and if you start downloading third-party applications you may accidentally receive malware that can then harm your device and steal your data.

Another tip is focussed on ransomware. It's been in the news daily and there's a nice simple solution to make sure you don't fall victim to it; backing up your data.

There's evidence of some security researchers decrypting ransomware strains but more often than not you have to empty out your piggy bank and pay the hackers.

A complete back up can get you out of a tricky situation, as long as it's stored on a secure device.

Phishing scams, much like ransomware, are an ever heightened trend that's emerging throughout the world.

Now I'm not talking about Robson Green claiming he's caught the biggest Marlin on his newest TV series, but the social engineering attack that targets people on a daily basis.

They often appear legitimate as they are from friends, family or a company that you already have a connection with but it's easy to verify the source before you click on a link or attachment.

There was an article in January about the most common passwords of 2016 and the main tip for Data Protection Day is to never reuse passwords.

Many people would use the same password across all of their accounts and devices.

This is a big no-no in terms of keeping your data safe. One hack into a Facebook account and then the rest of your accounts would be vulnerable.

All of these seem pretty simple and common knowledge, especially to people who work within a security focussed role.

Much like the whole product vs process debate that reigns on in the cybersecurity industry, it's all about educating people as much as possible.

That good old anti-virus protection you have on your laptop will do as much as it can to keep hackers at bay, but if you leave yourself open to attack, or don't follow the best practices when it comes to keeping yourself safe, your defence will deplete. Don't be a fool, secure your tool!

About The Author



My Name is the Jonathan Stock and I am a cybersecurity recruitment consultant working for IntaPeople. In addition to sourcing candidates for various cybersecurity companies.

I am also a contributor to several cybersecurity online magazines, a member of the UK Cyber Security Cluster and an event coordinator.

Jonathan can be reached online at j.stock@intapeople.com, [@JonathanStock86](https://twitter.com/JonathanStock86) and at our company website <http://www.intapeople.com>

Austrian Hotel's Ransomware Run-In Highlights IoT Vulnerabilities

By Alexandre Cagnoni



We're seeing it everywhere... from lightbulbs and refrigerators to cars and homes... the ongoing adoption of IoT (Internet of Things) in everyday items is on a trajectory with one speed: fast. But with that remarkable innovation comes some ever-increasing concerns.

IoT is meant to bring new levels of convenience and knowledge for both consumers and corporations. It arms us with new capabilities as well as countless clever

new insights on energy, food, security, transportation and health... just about everything. And even though IoT is on a speedy path to hit every aspect of our lives at some point, a recent IoT-related ransomware run-in at a hotel in Austria illustrates how IoT opens up new vulnerabilities that even stretch into remote mountainside retreats where people usually go to rid themselves of the usual stresses in life.

In late January, we learned that the nearly \$400-a-night Seehotel Jaegerwirt, located far in the Austrian Alps within the village of [Turracher Höhe](#), became one of the latest intriguing cases of IoT leading to a ransomware attack. The press was immediately abuzz with rumors of self-locking hotel rooms in the hotel. It turns out that was not exactly what happened. But we will also explain how that's only the beginning of the story.

Today, people can lock and unlock their home's front door using a mobile app, remotely turn on your car on a cold morning, control the temperature in your home or at the office... the applications are endless. It's all about convenience, but what about security? IoT's success is rooted in the assumption that only the intended or authorized user would interface with the IoT-enabled device or system. What happens if someone breaches the system that controls the various devices? Just one small example would be a Trojan being placed on a mobile device and thus gaining access to your seemingly benign devices that turn out to be not so benign once their controlled by someone else.

That's all too true when we see examples of vehicle brakes being remotely controlled by hackers. And last October the attack on Dyn created a major Internet outage – all from cybercriminals that used vulnerabilities on IoT devices. So not only are the devices themselves

open to attack, but they can be used as tools for attacks of a much grander scale. It was reported that ransomware was used to lock or unlock doors at that hotel in Austria, and the attackers demanded a ransom in bitcoins. The ransom was eventually paid, and it turns out their key card management system was indeed unavailable for a bit. It created a lot of inconvenience, but no one's hotel room actually became a temporary jail cell and no one was held captive.

Now think about the very, very near future, with the massive use of remote controlled devices, providing energy to homes, light, controlling cars, even getting access to airplane systems? A zero-day threat could cause potential damage to a whole city infrastructure. It reminds me of a "Two and a Half Men" episode where Walden and his partner develop software that causes a blackout across the entire country. Could this happen in the future? What about "Person of Interest," where Finch uses smart camera exploits and even laptop cameras in public coffee shops to spy on people? Are these really farfetched, or are they just around the corner?

IoT already represents a tremendous step forward in innovation, making our life easier, smarter, and connected. But both the typical consumer as well as the world's largest companies must not only acknowledge and learn about the associated risks, but they should also put processes and precautions in place to avoid misuse. Possible steps include:

- Remote controlled devices should not allow a product to begin functioning before a user changes the "factory set" administrator name and password.
- Firmware updates or app insertion should have a well-controlled system behind it, preventing unauthorized access.
- Eventual failures and attack detection should lead to an automatic safe mode, for example some form of manual or altered mode.

The hype surrounding IoT is huge, but the attacks surrounding IoT will undoubtedly become the bigger news maker. After all, when a lakeside resort nestled in the Alps hits the headlines for IoT related ransomware, it shows anything can be up for grabs. IoT is clearly going to become one of the new elements of crime. Makers of IoT devices and related systems must play a strategic role in educating the general public on both the benefits and the risks we take as the world depends more and more on connected devices.

About the Author



Alexandre Cagnoni is CEO of McLean, Virginia-based Datablink (www.datablink.com), a global provider of advanced authentication and transaction signing solutions.

The best practices in dealing with ransomware

By Milica D. Djekic

Our society is becoming dependable on new technologies in the both – legal and illegal connotation. The hacker's community is getting bigger and bigger and it's right time to take some actions on to appropriately handle those threats.

Combating the cybercrime is not an easy task – especially if we take into account how skillful and sophisticated today's security concerns could be. One of the most mature malware the black market is dealing with is ransomware. This sort of malicious application is well-developed and quite capable to lock your computer or some files and data being allocated within your IT infrastructure.

Through this article – we would talk a bit more about how those malware could get hazardous to anyone's systems and what some of the best practices in fighting this challenge could be.

What is the ransomware?

The ransomware is a computer's malware that is capable to lock your system or some files and data and in order to unlock them it seeks the ransom as a way of financial compensation. This sort of the malicious piece of software is the product of the cybercrime's underground and it literally works as a quite sophisticated blackmail machine. There are two main types of this malware and they are locker ransomware and crypto ransomware.

The cyber criminals dealing with this sort of a business would do that for a reason they would obtain the reliable source of incomes once they find the right targets. They would not get selective about their victims – they would target anyone being willing to pay the ransom. The average ransom on the black market is around \$300, while some common range of prices is between \$200 and \$800 per a file.

According to some sources – the total economical loss being caused with this sort of a cybercrime was more than \$24 million in 2015 and the next year the level of infections with this sort of malware increased by more than 500%.

Obviously – it's a huge concern to the entire legal environment. Also, we would mention that this type of malware would firstly get used in Russia and very soon it would get a threat in the western countries as well.

Today – the most threatened country being affected with this sort of product is the US being followed with the rest of developed economies.

The locker ransomware is able to lock your computers presenting itself as some Law Enforcement agency that found some concerning data on your computer and it would seek the money in order to unlock your machine. Many people dealing with this sort of message would experience some sort of the panic attack and they would so irrationally pay the required amount of a fine.



The real Law Enforcement agencies would always recommend to avoid paying such a blackmailing requirement, but people would get scared about their confidential data being allocated on that computer and they would give some money on. In addition, it's important to mention that the way of payment in this case would be a voucher that could get converted into the money using the well-known online cash machines that would seek your voucher's code in order to give you the financial compensation. Further, those incomes would get sent to fraudly created debit cards and in such a manner the criminals would launder that money.

The crypto ransomware is a cybercrime solution that would encrypt your files and data and seek from you to pay a fee in order to get a decryption key. It's quite interesting that people would willingly pay for this sort of blackmail – even no one would guarantee them that they would get anything in return if they pay that ransom. As a way of the payment – the cyber criminals would use Bitcoins. It's a quite common scenario that people would find some files being inaccessible and they would get a message that they need to pay a certain amount in Bitcoins.

So frequently – people would not even have their Bitcoin wallets and they would rush to open the one. We are quite confident that people reading this article would be familiar with this sort of threats and they would know that the targets would get a limited time to respond to the cybercrime's demands. Finally, it's clear that this sort of threat would need the certain steps getting applied in order to cope with this type of security concern. Some of the best practice recommendations would get provided through this effort as follows.

The preventive methods

The ransomware is a quite recent security challenge affecting the developed societies several years back. It's only one of the steps in a malware evolution and many experts would agree that it's a quite mature solution at the present. In other words, the cyber industry got a plenty of time to research this type of malicious code and develop some sort of response to it.

For instance, we would find some sources claiming that the entire anti-malware software would get capable to handle this sort of threat which is more than encouraging.

Also, we would deal with some web resources indicating that there are some tools being available online that could secure you from the ransomware attacks. In total, this would sound quite promising and we believe that the entire society would find a way to deal with this challenge.

It's especially beneficial that the majority of the Law Enforcement agencies would get more and more capable to handle this sort of crime, so we can expect in the future that those services would be able to resolve the majority of our concerns.

The role of good incident response

In case of ransomware threat – it's good to know that even if you are a victim of the cybercrime campaign – there are still the ways to respond to such a situation. For example, many experts would suggest that the best way to assure your IT infrastructure is to create its backup. You can do that using some physical devices or – as it's quite popular nowadays – using some of the cloud-based systems.

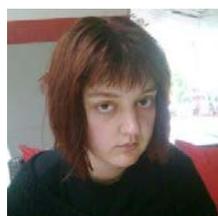
In this case – we would talk about the crypto ransomware attacks that would make your files and data getting locked. If you got the backup of your office – you would easily delete all the files being encrypted and recover your data applying the backup option. It's quite obvious that the backuping is one of the main best practice procedures that should get followed in any case.

The conclusions

The role of this effort is to provide a quite comprehensive insight into a cybersecurity challenge as ransomware is. We are aware of that this topic would get emerging nowadays, so please consider our article as something dealing with the new tendencies in the area of cyber defense.

Finally, the point would be that some future solutions would offer us the better opportunities in coping with the similar types of threats.

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.

Click here to get
20% off
your delegate pass

PAY **360°**
**DIGITAL
PAYMENTS**

AN ANNUAL CONFERENCE BY THE EMERGING PAYMENTS ASSOCIATION

23-24 May 2017, Coombe Abbey, Warwickshire

Themed around Mobile, Regulation and Banking, PAY360 Digital Payments is the forum to interact with PayTech's best thinkers.



30 TOP LEVEL
PAYTECH SPEAKERS

 **8 HOURS
OF CONTENT**

NETWORK WITH OVER
250 DELEGATES 

GALA DINNER
THE NIGHT BEFORE
THE CONFERENCE



Meet representatives from the big incumbents, existing challengers leading the charge, and everyone else trying to take a share of the market.

Speakers include:

Gijs Boudewijn, Chair Payment Systems Committee, The European Banking Federation

Sophie Guibaud, MD, Fidor Bank UK

Scott Manson, Head of Payment Strategy, Nationwide

Kirstine Nilsson, Strategic Engagements & Relationships, GPCM, Swedbank



@EPAassoc #EPADigital

Find out more about us emergingpayments.org/events

Achieving Digital Trust in a World of Data

By Drew Del Matto, Chief Financial Officer, Fortinet

Cybersecurity is at a critical tipping point. With massive volumes of data being generated and analyzed across the globe every day from a variety of sources and devices, an entirely new approach to network security is required. From both a business and a technology perspective, traditional security paradigms are struggling to be agile and fast enough to move at the speed required in this new world. How do companies successfully lead in a world that is being transformed by technology and the utilization of valuable data? The linchpin to success going forward will be a business's ability to flexibly secure its sensitive data and create digital trust with its customers and ecosystem.

Data is the fuel for the digital economy

The Internet of Things (IoT), heterogeneous data models, mobility, cloud solutions and analytical tools are driving the inexorable proliferation of data. Tremendous value and competitive edge are created through the effective use of data, and businesses across all industries are using it to transform themselves and generate net new revenue streams. Data has become the fuel of the next-generation business economy. We see examples of this every day.

Some of the most established industries, like healthcare, are now more data-driven than ever. Doctors have always used data to evaluate their patient's condition, but that data used to be stored on paper and film. Now it's more available; physicians can instantly share files, images and video with colleagues anywhere in the world, making doctors and the entire medical profession more productive and no longer bound by time or distance. Data can be correlated in ways never possible before, leading to more proactive diagnosis and treatment. And data accessibility has the added benefit of allowing patients to be more engaged in their own care.

Data is disrupting businesses as well. Uber is the world's largest point-to-point passenger service without owning a single car. AirBnB is one of the fastest-growing hospitality services without owning a single piece of property.

Companies like Google and Facebook are using consumer data to create new revenue streams and deliver better customer experiences. Data has become an invaluable currency, and businesses depend on it to fuel growth and innovation.

Data drives value creation and productivity

A recent report by McKinsey Global Institute (MGI), titled [*Digital Globalization: The New Era of Global Flows*](#), found that the flow of data between countries has brought the world closer together and made us all more productive. Global flows of all types (goods, services, finance,

people) drive growth by connecting economies. According to MGI's analysis, "over a decade, all types of flows acting together have raised world GDP by 10.1 percent over what would have resulted in a world without any cross-border flows. This value amounted to some \$7.8 trillion in 2014 alone, and data flows account for \$2.8 trillion of this impact."

The reality is that in order for data to fuel and transform businesses, information technology and security are the essential underpinnings to its ultimate value creation. Technology makes it possible to correlate, analyze and draw conclusions from data in ways never seen before. Every industry is looking for ways to monetize the data they uniquely own or can gather. Organizations must monetize data or they will be left behind.

IDC published its 2017 IT industry predictions, highlighting the accelerated transformation to a digital, data-driven economy. Some predictions include:

- By the end of 2017, revenue growth from information-based products will be double that of the rest of the product/service portfolio for one-third of all Fortune 500 companies. ([IDC FutureScape: Worldwide Digital Transformation 2017 Predictions](#))
- By 2019, 40 percent of IT projects will create new digital services and revenue streams that monetize data. ([IDC FutureScape: Worldwide CIO Agenda 2017 Predictions](#))
- By 2020, 50 percent of the Forbes Global 2000 (the world's largest public companies) will see the majority of their business depend on their ability to create digitally enhanced products, services, and experiences. ([IDC FutureScape: Worldwide IT Industry 2017 Predictions](#))

Clearly, the transformative potential of data is huge. Unfortunately, criminals see the value in data as well.

Cybersecurity in a data-driven world

Business priorities around cybersecurity have evolved in recent years to account for the changing threat landscape brought on by the increasing value of digital data. 2014 was dubbed the Year of the Breach, with sophisticated, targeted mega-breaches of customer and employee data at places like Target, Sony, eBay and Home Depot grabbing the biggest headlines. The following year saw the rise of stewardship and the role of the CISO, with business leaders responding in droves to the increasing threat and instituting new security policies and resources to protect their businesses from data theft. Bad actors got more creative and found new targets. Witness the massive data breach at the U.S. Office of Personnel Management (OPM), where background investigation records of more than 20 million current, former and prospective federal employees and contractors were stolen.

As cyber attacks worldwide increased in frequency and sophistication in 2016, the demand for highly skilled security talent also increased. The result was an exacerbation of the already

troubling cybersecurity talent shortage, estimated to be as high as one million open jobs. Organizations that recognize a need to build cybersecurity teams, and are prepared to spend the money to do so, are struggling to find the expertise to fill those roles. And now, as data is becoming exponentially more critical to future growth and innovation, the ante is going up again.

The trust side of the data coin

In this world where data is king, just as important as an organization's ability to use its data is its ability to protect it. Businesses experience value through additional or new revenue, lower costs or faster time-to-market. Customers experience value through new or better experiences, greater convenience and lower cost.

But in order for data to flow freely, and for companies to use that data successfully, it must be protected, and the company must be trusted. The more individuals believe that businesses will protect their data and use it for good, the more willing they are to provide it. The key to success in the digital economy is trust. Lose that trust, and the impact to your business can be crippling.

Building secured business offerings creates a trusted brand. Designing and building an architecture that is strong across the value chain ultimately creates digital trust.

This requires a shift in the approach to security, from reactive to proactive. Security is a business issue first. This includes not only appropriate investment in technology and architecture, but it requires starting with the mindset that security is paramount. If your security strategy is not integrated into your business priorities and initiatives right from the start, it will not serve the business well and will constantly struggle to keep up.

The reality is that cybersecurity is a business-wide issue and opportunity. And while the CISO is the quarterback, cybersecurity as a core behavior needs to permeate every function and all levels of an organization.

The CISO's challenge

The role of the CISO is changing. What began as a technologist or compliance expert role must now be a business leadership role first. CISOs must drive the shift in approach to cybersecurity to ensure that valuable data remains protected.

With the rise of the cloud and the growth of shadow IT, businesses often don't even know where they are vulnerable, where all of their data is, and if it is being protected. As new threats to our information security have emerged over the years, the result for most businesses has been siloed solutions. This endless cycle of "see a vulnerability, buy a solution to address it" results in a patchwork of products and capabilities that don't talk to each other or coordinate any kind of policy or response. This type of security infrastructure is complex and difficult to manage and does nothing to help the business to keep up with the ever-evolving cyber threat landscape. Security, in this model, becomes an inhibitor, not an enabler.

In order to succeed, CISOs must evolve their approaches across people, process and technology. Security must be embedded into the culture and made a priority for all members of the organization. Each individual must feel a sense of ownership and pride in securing the company's most important assets, and it must start at the top. It is also critical to invest in attracting, developing and retaining the right talent to ensure that the organization remains secure.

Creating and instituting the right processes spans taking regular assessment of all assets (you can't protect it if you can't see it) to regularly and proactively implementing fixes for "known" vulnerabilities or threats across the organization. According to a recent report by AT&T, 90 percent of the attacks they log are known attacks or their variants – not zero-day attacks. Security risk also needs to be evaluated and planned for in key business initiatives from the start – CISOs are uniquely positioned to play this role by effectively translating security requirements and capabilities into the language of business.

Lastly, CISOs must take an architectural approach to security. That doesn't necessarily mean scrapping everything and starting over. The reality is most organizations already have many different security devices, often from many different vendors. Deploying a truly integrated security fabric will let businesses maximize existing investments by pulling all of the discrete solutions together. The result is a collaborative system of tools that work together to monitor the network, share information and respond to threats, no matter where they occur. A truly integrated fabric also gives you visibility across your entire network, from endpoint devices through to the cloud.

At a time when our networks are under constant attack, visibility and end-to-end protection are critical. With increased network complexity and attacks becoming more sophisticated and targeted, an integrated security strategy is the only way to ensure that organizations achieve the digital trust required to fuel the data of today's global businesses.

About the Author:

Drew Del Matto brings more than 20 years of financial management experience and expertise in the network security market. Prior to joining [Fortinet](#), Drew held a variety of senior management roles at Symantec including acting chief financial officer, as well as senior vice president and chief accounting officer. Drew also served as Symantec's corporate treasurer and vice president of finance business operations, responsible for all treasury functions, various aspects of mergers & acquisitions, pricing and licensing, financial planning and analysis, and revenue operations. Prior to Symantec, Drew held senior finance leadership roles with Inktomi Corporation and SGI Corporation. He began his career as a CPA in public accounting with KPMG LLP.

New Attack with Seldom Used Vector

PowerSniff

by Charles Parker, II; Information Security Architect

Malware is being coded and released into the wild at an alarming rate. People from across the globe are coding this for personal profit, as a contract, or to prove a point (e.g. hacktivism). Usually these have been noted to operate in a narrow way.

The traffic to the target is through the email. The user reads the email with an attachment, opens this, and the malware is saved to the hardware. This mode has been repeated across the globe.

Recently there has been a new variant on an older method. This new variant saves the malware into the memory (RAM). This is distant from other currents, but has recycled an older method. A prior example of this attack was the Ursnif malware.

Fileless Malware

As noted generally the malware is saved to the hard drive. With this in effect, the malware is long-lasting in that when the computer is shut down, the malware is still present when the system is turned on.

With this new variant, the malware resides in the RAM. This is not stored on the hard drive of the targeted, infected system. This had been experienced more with drive by malware attacks. While this is unique, it has proven itself to be effective.

Usage

Historically, the attackers have not used this in a preponderance of the time. This was a less attractive option as the attack would fail as the user reboots their system, clearing out the RAM, and effectively removing the malware.

This does have a benefit in that AV is generally engineered to scan the hard drives and not the RAM.

Process

On a basic level, this is structured as a social engineering attack. This was not part of a spam campaign. Structurally, the person receives an email. This is personalized with the person's name, address, and other select information.

The body of the email indicates there is a pertinent rationale for opening the attachment presently (e.g. the user has to open the attachment urgently!). The email has in the body an

attachment of a Word document. Since this is not an .exe file, the person may have a better sense of security and the person believes this is fine.

The user then opens the word document. Unbeknownst to the user, this allows the macro in the Word document to execute. The malware is placed in the memory of the system.

This was also coded to check if the malware had been placed in a sandbox or virtual environment.

Targets

The Palo Alto Networks noted an estimated 1,500 emails were sent with this campaign. As further evidence, the email was specialized for each person.

The targets have been in the US and Europe, with a smaller portion of the emails being sent to Canada. This has focussed on the hospitals, manufacturing, energy, and tech industries.

Prevention

Malware has tended to be used repeatedly and re-surface when users and Admins have forgotten about it. This is a sample of malware that needs to be wary of and place defenses in place and not remove them for convenience.

There are a number of defenses for this. These are familiar and have been seen many times before with other instances. These common sense approaches still work well when implemented.

The user should not enable macros in the Word documents. If the user is not certain of the sender's identity or is not expecting an attachment, the attachment should not be opened.

About The Author



Charles Parker, II began coding in the 1980's. Presently CP is an Information Security Architect at a Tier One supplier to the automobile industry. CP is presently completing the PhD (Information Assurance and Security) with completing the dissertation. CP's interests include cryptography, SCADA, and securing

Charles Parker, II can be reached online at charlesparkerii@gmail.com and InfoSecPirate (Twitter).

INTEGRATION MAY ANSWER CHALLENGES IN MACHINE INTELLIGENCE

Bringing several functions together creates a stronger security posture

by Martin Korec, Head of Quality Assurance, GREYCORTEX, s.r.o

Introduction

You are probably familiar with terms “Artificial Intelligence” and “Machine Learning,” i.e. the idea that computers can be taught to learn, and then make predictions based on the data they are given. Artificial Intelligence and Machine learning tools present huge opportunities in many areas, especially in cyber security.

The UK government considers it technology which is the engine of the [digital revolution](#). But, some are skeptical. Gartner put Machine Learning (a subset of Artificial Intelligence) at the “[Peak of Inflated Expectations](#)” in its 2015 Hype Cycle. Simon Crosby of Bromium considers these tools to be a “[pipe dream](#).”

What Are Artificial Intelligence and Machine Learning?

Both Artificial Intelligence and Machine Learning address the capability of machines to be taught to make predictions based on “learned” data. Both are popular terms, and are [often confused](#). [Deloitte](#) has decided that a better term for their capabilities is “Machine Intelligence” - describing it as “*an umbrella term for a collection of advances representing a new cognitive era. We are talking here about a number of cognitive tools that have evolved rapidly in recent years: machine learning, deep learning, advanced cognitive analytics, robotics process automation, and bots, to name a few.*” I’ll use Machine Intelligence here (partly because “Artificial Learning” didn’t work as well) to mean the use of data analytic/predictive tools in the network security context.

The Benefits of Machine Intelligence are Significant

The essential benefit in Machine Intelligence is that it can take truly massive amounts of data, analyze it in real time, and identify anomalous or malicious behaviors invisible to manual review, or which would not be accurately identified through static detection rulesets (which are also a hassle to set up).

Of course, the more data a Machine Intelligence solution has, the more effectively it can do its job. Some have claimed prediction can be [improved by over 90%](#). If the solution has limited data, e.g. from only Netflow, it is limited in its effectiveness.

If input data comes from every layer of the network, then the Machine Intelligence solution can identify anomalies at each layer, and each device within each layer. This means the Machine Intelligence solution identifies behavior - like advanced persistent threats or insider attacks - that may be limited or very well hidden among massive volumes of network traffic, and which [would be missed](#) by a security team pre-programming logic in SIEM systems, even well thought-out ones (a [limitation of SIEM systems](#)), or working with an IDS ruleset alone.

Drawbacks are Claimed

Advanced analytics have been around for [20 years or more](#), there must be something wrong with them, or we'd all be using them. Right? Naturally, as with anything created by humans, Machine Intelligence solutions can be [defeated by other humans](#). However, there are several existing approaches, including classification algorithms, proven to successfully [mimic security analyst behavior](#) which can be used in design to detect and avoid defeat by new threat samples.

A second criticism of Machine Intelligence solutions is that they are [not “plug and play,”](#) e.g. that they need analyst time to filter out false positives/e.g. teach the system what is a threat and what isn't. Failure to do so leads to excessive false positives and alert fatigue. Alert fatigue is a problem. A [recent article](#) suggests that over half of security professionals are missing alerts they should address.

However, [MIT research](#) indicates that human/Machine Intelligence collaboration is actually beneficial and can reduce false positives by close to 85%. Furthermore, while Machine Intelligence solutions may not be “plug and play,” their implementation time is much lower as compared to SIEM systems (hours vs. months) and training the machine on false positives requires a very small actual time commitment (minutes a day).

Bringing Solutions Together

Is it possible to have the benefits of Machine Intelligence technology, but minimize the hassles? Is it possible to use Machine Intelligence in such a way that this technology is used for truly advanced analysis, reducing false positives and saving the security team's time?

Integrating several features/technology types into one solution mitigates several issues with Machine Intelligence technology, and creates a more efficient system. Specifically, integrating with IDS rules and network performance monitoring is an efficient means of improving network security by joining complimentary features and data sets.

Integration Brings Advantages

In such an integration, detection is more effective and false positives are reduced. Less time training the system is required, and information that is “trained” starts from a more accurate position.

Integration with an IDS ruleset specifically brings two benefits: The first is that the IDS, a list of existing rules and known signatures, helps the Machine Intelligence tools function more

efficiently, by determining early in the data analysis that certain traffic matches known malicious code or patterns, creating a deeper chance for analysis of events that do not trigger an IDS alert. Secondly, this type of integration has the added benefit of identifying for the Machine Intelligence tools what particular viruses/malware/trojans, etc., look like. This means that the predictive analysis tools have more, and more accurate data upon which to build their analysis. This data is also available much more quickly than if the solution was completely self-educating, or assisted only by the security team.

This also applies to adding performance monitoring capability. A more informed and more efficient Machine Intelligence solution exists because traffic data is integrated to help it spot things like too many communication partners, services which haven't been used before, exceptional network application delays, changed MAC addresses, or new devices or services in the network.

Integration also benefits the security team, because integrated IDS data increases efficiency. Not only does the team spend less time training the system (see above) but it also means more accurate results, resulting in less risk of alert fatigue. Alerts that actually matter are less likely to be missed as a result of the process.

In summary, Machine Intelligence technology, despite what its detractors suggest, is here to stay. Though all providers may not be using its full capabilities, its potential is too great, and its benefits in terms of detection of advanced threats too tangible for it to be given up. But, it can be improved.

An integrated approach; featuring several different types of input and analysis helps to streamline Machine Intelligence data analysis, making it more effective and improves the functionality of the integrated tools. This means more effective and more efficient network security, and more family time for security analysts.

About The Author



Martin Korec, is the Head of Quality Assurance at GREYCORTEX, s.r.o. He is brings six years of academic experience in data processing and information security at Masaryk University, as well as two years of experience in engineering security solutions and network security audits, both with GREYCORTEX, and Czech company Trustport.

He has published articles in the security journal [DSM](#). Martin can be reached online at (martin.korec@greycortex.com) and at our company website <http://www.greycortex.com/>



CYBER SECURITY FINANCIAL SERVICES EXCHANGE ASIA

14-16 May, 2017 • Bali, Indonesia

DID YOU KNOW?

In the second quarter of this year, cybercriminals tried to inject more than **1 million** malware programs into financial companies worldwide, a **50% increase** from the same period in 2015

- Kaspersky Lab

The global spending for cyber security was nearing **\$76.1 billion in 2015**—and that number is expected to rise to **\$170 billion by 2020**

- Gartner

54% of 540 businesses surveyed had come under attack from ransomware in the last 12 months. The most commonly targeted types of business were in the healthcare or finance industries

- Osterman Research

Financial services firms will need the highest increase in security spending to avert cyber attacks. Financial services companies would face the steepest increase in spending to reach an ideal state of protection — 13-fold rise to **\$292.4 million per company** to fend off **95% of cyber attacks**

- Deloitte

FIND OUT MORE ABOUT;

- The evolving threat landscape and which key technologies can **combat cyber crime**
- The latest cyber security **strategies and technologies**
- How other companies are making their **cyber security strategies work**
- How you can benefit from **pre-arranged and personalised schedule** of peer-to-peer discussions, business meetings, masterclasses, think tanks and conference sessions

Come be a part of Cyber Security Financial Services Exchange Asia 2017, 14-16 May in Bali, Indonesia, as we bring together 40 CIOs, CISOs and Heads of Cyber Security.

If you would like an invitation to see if you qualify as a delegate, email enquire@iqpcexchange.com referencing CDM_Del

If you would like to offer solutions to these Heads of Cyber Security, email enquire@iqpcexchange.com referencing CDM_Spex



CyberSecurity: Machine Learning + Artificial Intelligence = Actionable Intelligence

by Smit Kadakia, Co-founder, Seceon

Overview

The goal of artificial intelligence is to enable the development of computers to do things normally done by people -- in particular, things associated with people acting intelligently. In the case of cybersecurity, its most practical application has been automating human intensive tasks to keep pace with attackers! Progressive organizations have begun using artificial intelligence in cybersecurity applications to defend against attackers. However, on its own, artificial intelligence is best designed to identify “what is wrong.”

For today’s enterprise, that’s only half the challenge for defending against attackers. What today’s enterprise needs to know is not only “what is wrong” in the face of a breach, but to understand “why it’s wrong” and “how to fix it!” By combining artificial intelligence with machine learning to analyze and interpret actions and behaviors to predict attack patterns and recommend actions to stop threats in motion, technologists have devised a means to generate *actionable intelligence*. This article will seek to explain how artificial intelligence and machine learning can be used to practical effect in defending the enterprise in real-time.

Introduction

Machine Learning (ML) and Artificial Intelligence (AI) have been around in one form or another since the latter half of last century, but have picked up significant pace and applicability to change our day to day life in the last few years. The data science which now includes both ML and AI, among other things, has taken off on its own to become a major discipline in the educational world.

Business stakeholders have also recognized the importance of this discipline and have been leveraging contemporary data science methods to mine valuable information, make smarter business decisions and explore new opportunities using existing or newly harvested information.

The internet and mobile revolution of the last few decades have helped generate volumes of valuable information with potential to derive critical behavioral and structural insights from its collection. Naturally, the information gathering was vastly helped by the

highly connected world of people, the devices that they use and the mechanisms that facilitate collaboration on both a professional and social level. However, along with such benefits comes the dark side of exposing this information, leaving it open to bad elements of society for unintended use, such as financial exploitation through ransomware and malware types of cybersecurity attacks.

In the face of these attacks, technologists have begun developing a combination of cybersecurity defense techniques that rely on the collection of large volumes of real-time network, application and user interaction and behavioral data. This mix of data science techniques is the crux of how ML and AI disciplines can be leveraged in cybersecurity for proactively thwarting such attacks.

So, how are ML and AI different? How do they leverage interaction and behavior, and why is this important?

Machine Learning can be broadly defined as a focused approach of math and statistics-based algorithms that are designed to improve the performance of specific tasks through experience or learning that may or may not be easy to do by humans. On the other hand, Artificial Intelligence can be defined as a focused engineering approach for computing machines to do the tasks that we as people can do quite naturally, but conduct them without mistakes and, sometimes, much faster.

Andy Veluswami of Change.org expresses a visionary insight as, “We’re going to have a day, and I hope it’s soon, where machines aren’t just smart, but they’re also wise – and they have a context. Once we start getting there, and we already are, we’re going to start making a lot more progress.” We all intuitively know that this change is happening all around us, however, the practical aspect of this development, such as translating learning into “Actionable Intelligence,” is a key requirement that today’s cybersecurity practitioner must have.

So, how do we define what is and is not actionable intelligence in cybersecurity defense?

In the study of Machine Learning, the focus is on supervised and unsupervised learning. (We will not be considering deep learning in this article.) Supervised learning and many aspects of unsupervised learning require the known anomalies to be available to learn from and then predict anomalies in test data using the trained models and then fine tune them through techniques such as cross-validation. In cybersecurity, one is usually looking for an anomaly in the midst of a huge amount of normal traffic or behavior. Such a characteristic makes the anomaly detection a very difficult problem—like finding

a needle in a haystack. Furthermore, it is unrealistic to expect that training with anomalous data points in one industry, say eCommerce, is applicable to another one such as a healthcare datacenter. Additionally, modern attacks are more sophisticated and they hide themselves among many false attacks to defeat threat detection systems. Such complexity makes identifying anomalous training data points for all target industries a huge uphill battle. Lack of or difficulties in obtaining training data points make unsupervised learning a necessity in the world of cyber defense.

Given that unsupervised learning is required for such environments, one has to think through its pitfalls, recognizing that the prediction of the anomalies does not increase false positives or compromise accuracy. Various measures are used to assess the confusion matrix for accuracy, sensitivity etc., such as the Matthews Correlation Coefficient, however, it is not easy to consistently get good measures from the matrix in practice, demonstrating that more than just Machine Learning is needed to get to the desired results. There are various approaches that one can take, but the end result has to be the actionable outcome from the algorithms with minimal noise. This is where AI comes into play.

In April 2016, researchers from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) demonstrated an artificial intelligence platform called AI² that predicts cyber-attacks significantly better than existing systems by continuously incorporating input from human experts. The premise behind the finding is that it only needs an unsupervised suite of algorithms with feedback from expert security analysts to develop an AI-based algorithm that will detect the threats accurately. This too is a good approach, but these expert security analysts' services come at a significant cost, both in terms of time and money.

Furthermore, many of the ML algorithms indicate the threats long after they have been introduced and have taken advantage of the vulnerability. For example, a clustering algorithm may detect a threat after analyzing a history of patterns and indicate that the anomaly that occurred has been introduced in the network or a subnet sometime back in history. These threat findings are useful once you deploy an army of security ops staff to then hone in on the root cause for the anomaly and then address it. This sounds well and good, but the anomaly may already have spread by the time the security ops staff identify the root cause, requiring much wider investigation with increasing budget and delayed response time.

Clearly, it is desirable to identify the threat that occurred in real-time as soon as it happens, as well as provide the specificity about where it occurred. Furthermore, the method of arriving at this conclusion should also be provided for added benefit of

understanding and quick action to address the root cause. Such actionable intelligence must reduce the skill set required to address the threat. Moreover, in a highly developed system, it must eliminate the need to engage a human, offering the intelligence just-in-time to prevent any further damage, reducing the time it takes for a corrective action or a good combination of all to minimize the operational cost while setting the organization ahead of the attacker's plans.

Inherently, such an actionable intelligence must instill confidence in the user in preventing future attacks by learning from the attack and the response behavior. The real-time actionable intelligence should not only help in quick analysis, but should also help the organization learn from the intelligence much more rapidly and thoroughly so as to develop a better defense against not-yet-seen attacks as well.

We operate in an era where such systems are now in development with enterprising startups and vendors and are available in its early form. The advent of big-data platforms and related technologies are making this all possible. These systems are expected to dominate the cyber defense efforts of many of the elite organizations around the world and will be writing the next chapter in the forefront of cybersecurity. Genevieve Bell, Senior Fellow Vice President, Corporate Strategy Office, Corporate Sensing and Insights of Intel said in one of her recent presentations, "AI is the next big wave in computing. Like major transformations before it, AI is poised to usher in a better world." The signs are all around to take us there.

About the Author



Smit Kadakia, Co-founder, Seceon

Smit leads Seceon's data science and machine learning team, focused on developing a state of the art behavior anomaly detection solution.

Smit holds a B.S from VJTI, Mumbai; an MS in Computer Science from Indian Statistical Institute, Kolkata; and an MBA from Southern New Hampshire University, Manchester. Smit and the team at Seceon have built the industry's first and only fully-automated threat detection and remediation system using a combination of machine learning and artificial intelligence techniques.

Seceon's approach includes analysis of all traffic, flows and processes in and out of the network and correlates them near-simultaneously with behavioral analytics, recognized and zero-day exploits and policies to surface threats and proposed responses in near-record real-time. To learn more visit <http://www.seceon.com>.

(ISC)²



SECURITY CONGRESS

APAC 2017

03 - 04 July • Hong Kong

LEADERS OF TOMORROW

At (ISC)² Security Congress APAC 2017, you'll get to join thought leaders, (ISC)² Asia-Pacific Advisory Council members, (ISC)² Chapter leaders and over 350 InfoSec professionals for 2 days of knowledge sharing, strategic insights and networking with your peers.

50+ Speakers

2 Days

6 Tracks

35+ Sessions

Why Attend?

Invest in yourself in 2017

Learn the latest strategies and techniques to address cyber security threats

Meet regional experts & influencers face-to-face

Enjoy a customized learning journey

Earn up to 16 CPEs

Register Today & Save!

Early Bird (Before April 30): **US\$ 306**

Regular Price: US\$ 360

5% additional discount for group purchase.

For Inquiries: (852) 2850 6953

securitycongressapac@isc2.org

Tracks Include:



Cloud Security



Critical National Information Infrastructure (CNII)



Emerging Technologies & Security



Governance, Regulation & Compliance



Professional Development



Security Operations

Visit apaccongress.isc2.org

#ISC2congressAPAC

In Partnership with:



Supported by:



Platinum Sponsor:



Gold Sponsors:



Silver Sponsor:





How Passwords Are Hacked

IF A HACKER IS SOMEONE YOU KNOW (A FRENEMY):



They might be able to guess your password (dog's name, kid's name, etc.)



They may also be able to access your account if they know the answers to your password recovery questions

IF A HACKER IS UNKNOWN:



A brute-force attack is the most common strategy for cracking passwords



The program systematically tries every password combination until it gains access



The simpler the password is, the easier they're able to gain access

Most Common Passwords

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- solo
- passw0rd
- starwars



The Art of the Difficult Password

K5,747.;Sj24f9m/

-UP8cjCS!`S8'rA8

sP5}V,7^Wru&E:!

Include:

BY0gkeJBjBkS

Upper and lower cases

142369281258

Numbers

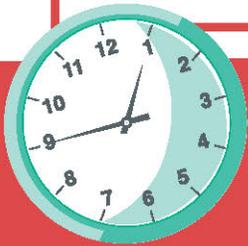
!@#%^)\$%#

Symbols

At least 16 characters

Don't include:

- Dictionary words.
- Usernames or IDs.
- Repetition.
- Any predefined number or letter sequence.
- Your birthday.
- People's names.
- Personal information (license plate number, phone number)
- Words or phrases from popular culture (Ihaveadream; Game_over,_man!).
- Dictionary words with simple algorithms applied (backwards spelling, combining words with punctuation in between).



How Long Would It Take?

The number of characters increases the number of possible combinations a hacker has to try; choose a very long password rather than a short, complex one

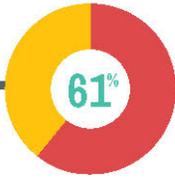


Password complexity also determines the length of time it takes to crack – a password with an 80-bit strength takes years longer to crack than a 30-bit password

april	Instant
april!	100 milliseconds
april10	2 seconds
april10!	19 minutes
apr&il10!	16 hours
Apr&il10!	4 weeks
A.pr&il10!	53 years
A.4pr&il10!	5,000 years
A.4pr&i#l10!	485,000 years
A.4pr&i#l1L0!	47 million years
A.4pr&i#l1L0!7	429 billion years



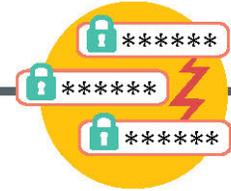
Having the Same Password for Multiple Accounts



61% of people admitted to using passwords on multiple accounts



When one company has a data breach, your other accounts can be compromised if you re-used the same password



In 2016, Mark Zuckerberg's LinkedIn, Twitter and Pinterest accounts were hacked; he was using the same password for all three accounts. Don't be Mark Zuckerberg.



How to Keep It All Straight

With many complex passwords for your many different accounts, how can you keep it all straight?



Some experts suggest using a phrase as a keycode:

"The 5-and-10 is at Main and Ash Streets"

→ T5&10i@M&ASt.s

Your favorite song is Madonna's La Isla Bonita, which spent 11 weeks at #1 on the music charts in 1987

→ LalsBo11#187!.



Use a password manager, a tool that helps you manage your passwords



Store passwords on a USB thumb drive



Go low-tech and write your passwords on paper or Post-its; it's less risky than:

- Using the same password at multiple sites
- Re-using old passwords
- Using easy-to-guess passwords
- Letting your software remember your passwords
- Not frequently changing your passwords

What Else Can You Do?

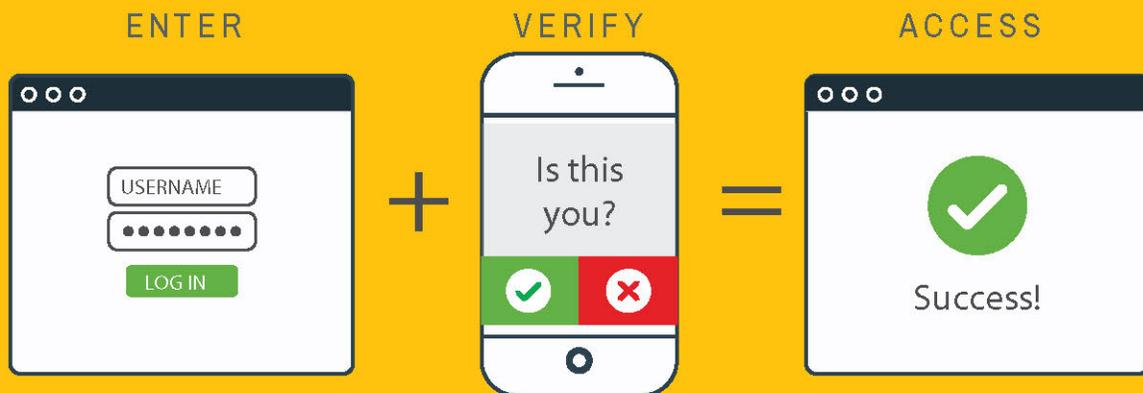
Don't use services with bad security

How companies store your password

- ** Plain-text password storage systems
Your password is easily accessible if the site gets hacked – Your strong password does not matter
- ** Basic password encryption systems
Hackers who gain access to the site can easily decrypt all passwords once they decipher the key – Your strong password does not matter
- ** Hashed password systems
Hashing a password is a kind of encryption that cannot easily be unhashed into the original password
- ** Hashed passwords with a dash of salt
Hashed passwords are stored with random characters added to the beginning and end, creating more complexity for hackers to decipher – LinkedIn was famous for **not** using salted hashes before its 2012 security breach
- ** Slow hash systems
Use algorithms that cause brute force attacks to take much, much longer, thus adding an additional layer of security

Use Multi-Factor Authentication

Two-step verification process that does not rely solely on a password



A one-time random security code is sent via:

- SMS message
- Phone app
- Auxiliary device, such as a token or smart card
- Secondary email address

1
2

Google, Facebook, and many others offer a two-step verification process



After a massive breach at the Office of Personnel Management, two-factor authentication increased from 42% of computers to 97% as part of a security initiative

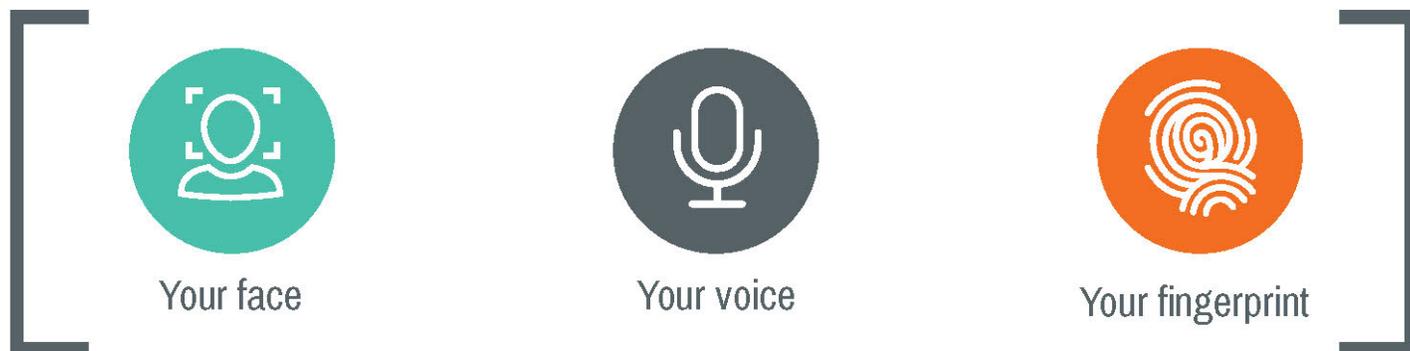


This additional layer of security means the hacker needs both your password and the security code to access your account

Biometrics

Many businesses are adding biometric authentication to their accounts

Biometrics require something that's unique to you:



Technology has made this easier than ever before to implement:

-  Cell phone touchscreens can become fingerprint scanners
-  Computer or phone microphones can allow for voice authentication
-  Webcams or phone cameras can become facial recognition devices

Why people are choosing biometrics:

-  Complex authentication schemes can prohibit higher security as users look for shortcuts
-  Biometrics are easy to use and therefore are met with less frustration — no more complicated protocols

Biometrics are currently used by millions of customers:

- Bank of America
- JPMorgan Chase
- Citigroup
- Wells Fargo
- PNC

Today's Threat Landscape Requires Adaptive Security

By Dan Joe Barry, VP Positioning and Chief Evangelist at Napatech

Cybercriminals' ingenuity seems to know no bounds. Their latest brainchild is the non-malware attack. In this scenario, no malware is downloaded to the user's computer. Instead, a malware script is activated that exploits vulnerabilities in flash, web browsers and other existing tools on the computer. As many of the security prevention solutions installed are focused on preventing malware download, this attack nullifies the effectiveness of a large part of the security architecture.

The onslaught of cyber threats shows no signs of slowing. Fortinet's [Global Threat Landscape Report Q4 2016](#) revealed an average of 10.7 unique application exploits per organization, and about nine in 10 organizations detected critical or high-severity exploits.

Not all of these threats are new; 86 percent of firms registered attacks attempting to exploit vulnerabilities that were over a decade old. In addition, 36 percent of organizations detected botnet activity related to ransomware, with an average of 6.7 unique active botnet families per organization.

Joining forces with time-tested attack methods, multiple recent factors have converged to create greater complexity and threat opportunity in the network, undermining the effectiveness of security prevention solutions. Bring Your Own Device (BYOD) can act as a Trojan horse to gain access to the network, and employees or contractors can knowingly or unwittingly mishandle data in a way that results in a breach. Cloud computing also provides new opportunities for attackers, who are constantly looking for novel ways to breach the wall by exploiting vulnerabilities.

Not Just Prevention – Detection

So then, in addition to today's security prevention solutions, organizations need a layer of advanced threat detection that can be deployed based on user and network behavior analysis.

These internal advanced threat solutions rely on continuous monitoring of network activity to first establish a profile of normal network behavior and then compare real-time activity to this profile to detect anomalous behavior. When used in conjunction with the information from other security solutions, it can provide the first indication that a breach has taken place.

Because it does not rely on detecting file downloads but on detecting activities that are out-of-the-ordinary, giving the security team the basis for further investigation, this solution is particularly effective in combating non-malware attacks. The fundamental capability underlying network behavior analysis is the ability to analyze all network traffic in real time. This requires packet capture solutions that can deliver each and every packet for analysis without packet loss, even at speeds up to 100G.

Recreating the Past

The majority of breaches—70 percent—are detected by third parties, The Ponemon Institute has found. This is the call that every C-level executive dreads, and the immediate concern is to determine the extent of the breach and the company's exposure.

The C-level executive will expect the security team to be able to report exactly what happened, when it happened and why it happened within a matter of hours.

At issue is the fact that the majority of today's security solutions are built to prevent and detect solutions in real time or at least near-real time. The ability to reconstruct the anatomy of an attack in detail is often impossible, especially if the attack took place up to six months ago.

There is therefore a strong case to be made for establishing the capability to record network traffic in a way that will allow the reconstruction of a breach even months after the fact.

The solution is a network recording or packet capture-to-disk capability, which allows every packet on the network to be recorded at speeds up to 100 Gbps, but can also provide multiple security analysis applications access to the same data. This allows deep-dive analysis of reliable network data on demand to support near-real-time forensic analysis or analysis of breaches several months in the past.

Learning to Adapt Security

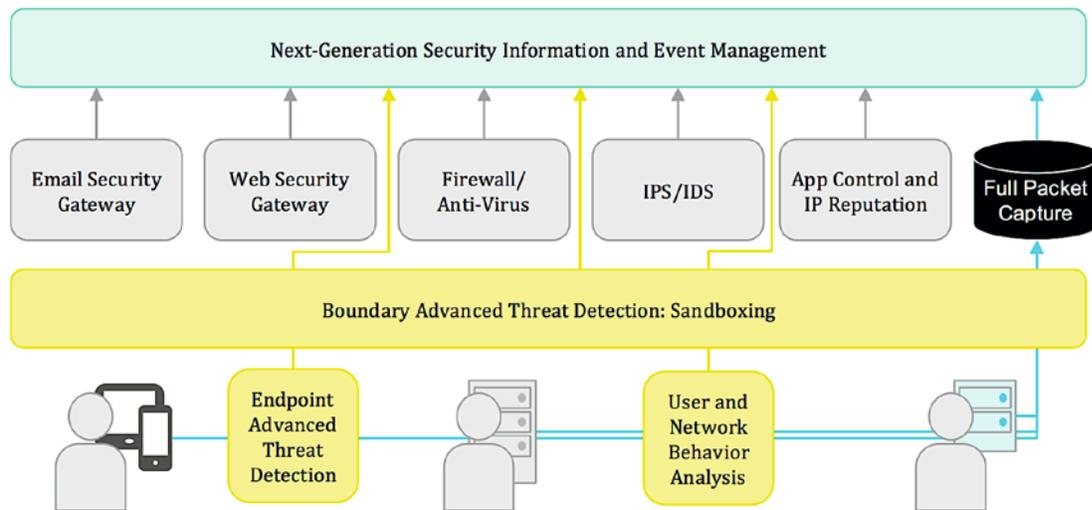
Gartner discussed the idea of an adaptive security architecture in a recent [report](#), concluding that there is an over-reliance on security prevention solutions, which are insufficient to protect against motivated, advanced attackers. The alternative proposed was an adaptive security architecture based on the following critical capabilities:

- Prevention to stop attacks
- Detection to find attacks that have evaded preventive capabilities
- Retrospection to react to attacks and perform forensic analysis
- Prediction to learn from attacks and industry intelligence to improve capabilities and proactively predict potential new attacks

What enables all of these capabilities and creates an adaptive security architecture framework is the ability to perform continuous monitoring and analytics, including network monitoring and analysis.

The Whole Security Package

By gathering together advanced threat detection solutions with next-generation SIEM solutions and packet capture capabilities, the stage is set for the infrastructure to support an adaptive security framework:



Such a framework enables the prevention of known attacks, detection of zero-day threats and detection of anomalous behavior that can indicate breaches that have circumvented defenses. The alerts and information from each solution are correlated and condensed by solutions like security information and event management systems that will enable security teams to quickly focus their attention on the most important threats.

The threat landscape is such that no one category of solutions will do. Organizations need to both prevent and detect the many complex attacks against the network. A comprehensive view of network activity is possible when security prevention and detection solutions work together. An adaptive security architecture is one that can record network data for near-real-time forensic analysis and post-breach analysis, providing the network visibility needed today to combat advanced threats.

About the Author



Daniel Joseph Barry is VP Positioning and Chief Evangelist at [Napatech](#) and has over 20 years' experience in the IT and Telecom industry. Prior to joining Napatech in 2009, Dan Joe was Marketing Director at TPACK, a leading supplier of transport chip solutions to the Telecom sector. From 2001 to 2005, he was Director of Sales and Business Development at optical component vendor NKT Integration (now Ignis Photonyx) following various positions in product development, business development and product management at Ericsson. Dan Joe joined Ericsson in 1995 from a position in the R&D department of Jutland Telecom (now TDC). He has an MBA and a BSc degree in Electronic Engineering from Trinity College Dublin.

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

SECURITY & COUNTER TERROR EXPO

PROTECT | PREVENT | PREPARE

3-4 MAY 2017 OLYMPIA LONDON

Supported by



Home Office

The UK's Leading National Security Event

Understand and protect against the latest threats



350+
Leading exhibitors



100+
Free-to-attend conference sessions



3,000+
Products & services on display



50+
Live demonstrations



10,000+
Senior security professionals

Register free at www.sctx.co.uk/cyber

Follow us on @GCT_EXPO www.sctx.co.uk/linkedin

Co-located with



Sponsored by

Organised by

Shedding the Light on Deep Network Visibility for Cyber Intelligence Applications

DWDM is the backbone technology for optical networks but presents a challenge to government agencies with intercept responsibilities.

Mike Seidler, Senior Product Manager, NetQuest Corporation

Dense Wave Division Multiplexing (DWDM) networks provide the capacity to carry the data of the internet and the long distance reach to span the globe; they have forever changed the way the world builds communication networks. Carriers all over the world are deploying Metro, Regional and Long-haul DWDM networks connecting their OTN, Native Ethernet and legacy SONET/SDH networks.

Traffic growth is the underlying driver for 100G+/100G/40G DWDM network transports and today's DWDM systems are closing in on supporting terabits of data per second over a single optical fiber.

These optical networks represent a tremendous cyber intelligence opportunity for national government intelligence agencies; however, intercepting and monitoring traffic carried over DWDM networks presents numerous challenges.

These challenges can be broken down into three significant areas: Access, Discovery and Big Data.

Access

Traditionally, government agencies would choose to avoid directly tapping the DWDM network and instead find a more convenient and less expensive access point in the long haul system.

By avoiding the DWDM network, standard analytic tools can typically be leveraged without having to first unravel all the wavelengths and underlying transport protocols within a typical DWDM signal.

Avoiding the requirement for DWDM network access is becoming increasingly challenging as the deployment of DWDM networks expands beyond backbone, subsea and long-haul applications and the number of active wavelengths grows to the current standard of 96 per fiber.

Physical space has also provided access challenges in the past as a combination of test and transport gear has traditionally been required to tap into an individual DWDM fiber link and process each of the wavelengths.

Discovery

Government intelligence agencies are often required to monitor networks that are not under their primary control. Under these circumstances, in order to provision a traffic monitoring solution, wavelengths captured from a DWDM network must be decoded to reveal the potentially complicated mix of transport protocols and traffic types that exist on the targeted wavelength.

This includes the discovery and reporting of OTN signals encapsulating channelized OTU4/3/2/2e, SONET/SDH signals including OC-192/STM-64 and OC-48/STM-16, as well as native 100/40/10G Ethernet flows.

An example of the potential complexity of a common transport signal carried over just a single DWDM wavelength is shown in Figure 1. The discovery process could take weeks of effort for just a single DWDM fiber pair.

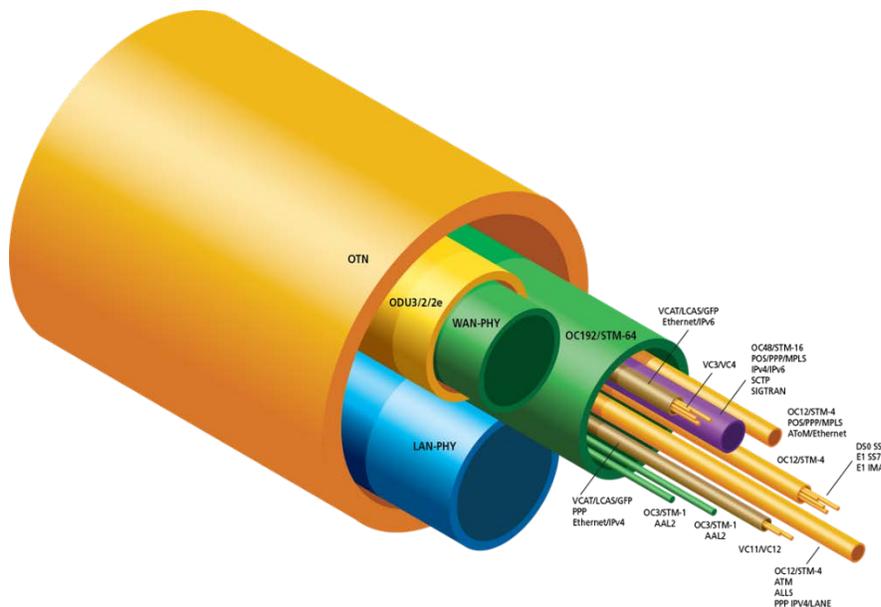


Figure 1: Optical networks can hide a complex transport architecture that makes gaining visibility into the data being carried extremely difficult.

The discovery process is additionally complicated by the constant evolution of the transport network and shifts to the mix of protocols and traffic types.

Network service providers are frequently turning up new wavelengths and the advent of software defined networking (SDN) is enabling innovative methods for instantly re-provisioning the network to address dynamic bandwidth needs.

This flexibility is a tremendous feature for the service providers but further complicates the intercept mission.

Big Data

Once the architecture of the target network has been discovered, the task of processing the traffic begins. However, as DWDM networks approach terabit speeds, this can translate into an untenable amount of data to process.

The vast majority of this 'Big Data' on the DWDM fiber link is typically not of immediate interest to government agencies and hence the ability to narrow the scope of data being forwarded to costly network analytic tools for deep packet inspection can be extremely beneficial.

Traditional Solutions

Monitoring a DWDM network typically requires the use of many pieces of standard transport and test equipment such as protocol analyzers, spectrum analyzers, routers and ROADMs.

The precise components can be difficult to identify but are typically sufficient to access, discover and handle the big data found on any individual wavelength as shown in Figure 2.

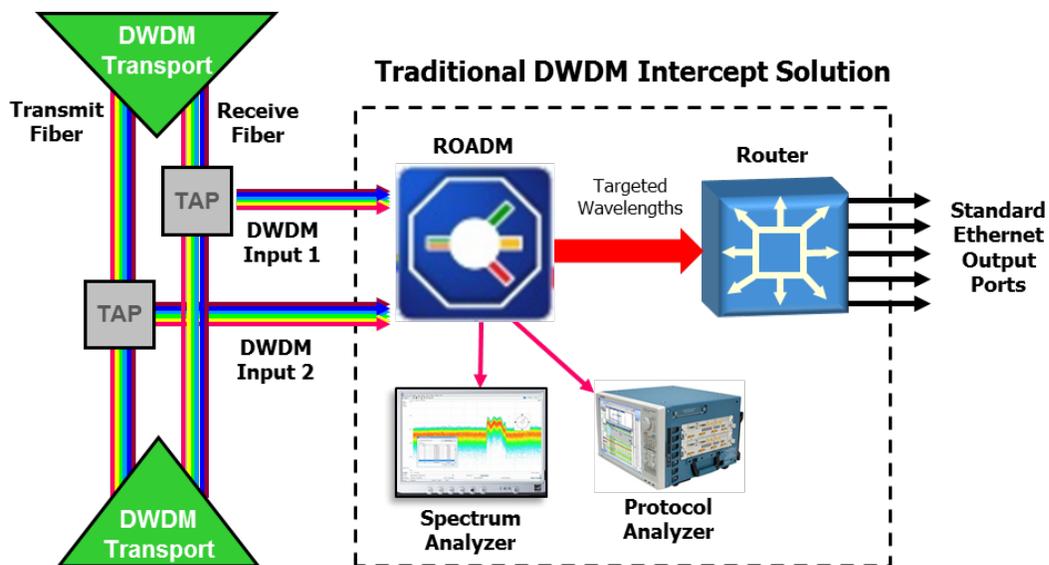


Figure 2: Traditional DWDM intercept solutions require combining many different pieces of costly transport and test equipment

The mix of required equipment is further complicated by the varying speeds of each of the wavelengths which can range from 2.5G up to 100G+ bits per second. Additionally, any changes to the number of active wavelengths or an upgrade to bandwidth capacity over any single wavelength could also require a costly upgrade to the necessary equipment.

Configuring and maintaining the infrastructure needed to monitor the DWDM links in modern optical transport networks is time-consuming and typically requires a large amount of expensive manual labor to operate effectively.

Multiple international government agencies have confirmed this time-consuming process can take weeks to complete the DWDM network discovery process alone.

Emerging Solutions

Innovative network intercept solutions are using advanced technologies to automate many of the aforementioned processes in an integrated solution. An integrated DWDM monitoring solution using standardized technology such as Erbium Doped Fiber Amplifiers (EDFA), Optical Channel Monitors (OCM), Wavelength Selective Switches (WSS) and the latest in programmable HW lowers the cost and significantly simplifies the management challenge.

Figure 3 shows how these components can be used in an integrated monitoring solution to access individual DWDM wavelengths, discover each wavelength's traffic profile and intercept specific data of interest.

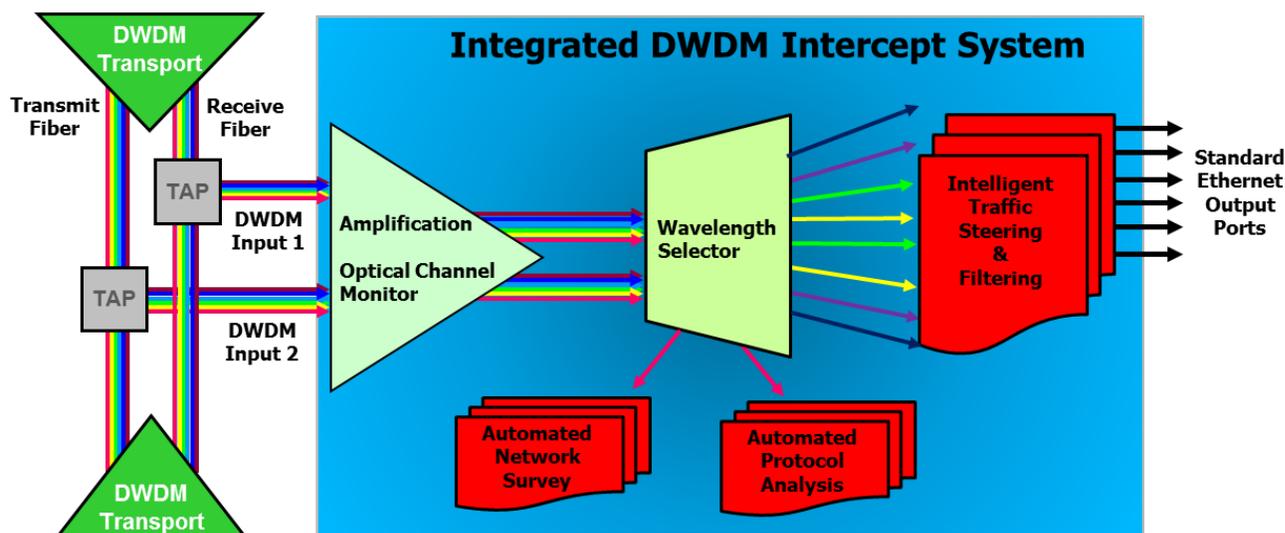


Figure 3: An integrated approach to DWDM intercept simplifies the automation of the monitoring process and maintains constant surveillance.

The integration of these elements into a purpose built solution simplifies the automation of the critical monitoring processes and eliminates the manual network discovery and mapping required in traditional solutions.

An integrated DWDM intercept solution will scan the traffic protocol mixes and alert cyber intelligence operators to any changes to the monitored network so critical surveillance is constantly maintained.

Conclusion

DWDM networks present a difficult challenge to government intelligence agencies tasked with cyber surveillance.

The complex traffic analytic tools used for critical cyber applications require a flexible and automated network access methodology that enables rapid and continuous discovery of the network architecture and its numerous traffic flows.

Traditional DWDM intercept solutions require several separate components resulting in high costs and inefficiencies and are challenged to react to changes in the targeted network. Integrated systems present an opportunity for a cost-effective automated solution that quickly discovers the fiber network architecture and steers the traffic flows of interest to the appropriate analytic tool while instantly reacting to any changes to the monitored network.

DWDM remains the backbone technology of the internet and intercept solutions must advance as quickly as the optical technology does in order to ensure the effectiveness of critical cyber intelligence missions.

About the Author



Mike Seidler is a senior product manager for NetQuest Corporation where he directs development of the company's automated intercept access and intelligent monitoring solutions.

Prior to his current position, he was a product manager for ARRIS and a principal hardware engineer for Motorola.

Mike can be reached at mseidler@netquestcorp.com and via NetQuest's corporate website at <http://www.netquestcorp.com/>.



4th Government Modernization IT

Focus Day: April 26, 2017 • Main Conference: April 27-28, 2017
Washington, D.C.

The CIOs Path to Modernizing Federal IT:
Maximizing Return of Investment. Improving Efficiency and Effectiveness.
Eliminating Security Threats.

Presentations from **12+ CIOs** of U.S. Departments



**CONGRESSMAN
WILL HURD**
U.S. Representative



RENEE WYNN
CIO
National Aeronautics and
Space Administration



FRONTIS WIGGINS
CIO
U.S. Department of State



JONATHAN ALBOUM
CIO
U.S. Department of
Agriculture



KIRIT AMIN,
CIO
U.S. International Trade
Commission



ANN DUNKIN
CIO
County of Santa Clara,
California



JOHN OWENS
CIO
U.S. Patent
and Trademark Office



JOSEPH KLIMAVICZ
CIO
U.S. Department of
Justice

Co-Located With Military Network Modernization 2017

Are you an active member of the U.S. Military and Government? Join us at NO cost



REGISTER TODAY! www.GovernmentITModernization.lqpc.com • 1-800-882-8684 • ldga@ldga.org

Office Depot

Allegedly Creative Vulnerability Diagnosis

by Charles Parker, II; InfoSec Architect

Retailers do not have the most pleasant sets of responsibilities. There are pressures from the staff, management, corporate office, and customers. There may be a mismatch viewed with what is sold and revenue, in that the goods and services may last for multiple years, while the revenue from the sale only appears in the first year, and the sales budgets continue to climb.

For instance, a customer may purchase AV with a three year time span now or a Mac Air. These last multiple years and are not recurring expenses for the consumer, while the expected increase in revenue has to come from somewhere.

At times, the management may feel the need to work within the grey area of sales to secure the transaction. This may not be ethical in its entirety. An example of this may be considered in 2008 when Circuit City filed bankruptcy. Up until the end, the store warranties were sold to consumers without the disclosure of the potential filing.

Post-bankruptcy filing and store closings, the stores were not able to service the products under their warranty, in comparison to the manufacturer's warranty. Others have elected to take this a bit further.

Office Depot's Allegedly Questionable Practices

The massive base of non-IT consumers provide a very large customer base to target and sell goods and services to. For the most part, this segment of the economy has much to learn.

The consumers have read a headline regarding a breach, however their IT and InfoSec knowledge base tends to be rather shallow, naturally with variances per person.

Due to the Office Depot being directly involved with selling computer systems and related services to this market, the staff members should be acting in a fiduciary capacity. They are the subject matter expert (SME). If consumer Joe has an issue with his computer, he may simply unplug the laptop and take the equipment into the local Office Depot for advice.

The systems are scanned by the Office Depot application. Allegedly the Office Depot's tech teams then informs these customers there is malware on the customer's computers when there is not. Although this generates revenue, it is not exactly prudent..

The staff was allegedly being pressured to sell computer protection plans per a news story by KIRO in Seattle. This was per a prior employee who was now a whistleblower. This Washington example however is not isolated.

This treatment of customers was also reported by WFXT in Boston. With the Boston case, there was also the same false positive report by the Office Depot staff members.

Sample

In following the scientific method of research, KIRO staff members purchased six new computers. These were unboxed and brought to the Office Depot for a PC Health Check.

After asking a few questions and scanning the computer, the “customer” was told by the Home Depot tech, in four of the six systems, their computer showed “symptoms of malware”. The tech diligently attempted to sell the “customer” the services to fix the computer, costing from \$149 to \$199.

To validate the brand new, directly out of the box computers did not actually have malware, the systems were brought to an InfoSec firm, IOActive. The report from the actual SMEs was the systems did not need any repair services.

Per the KIRO news story, the workers were told to sell the programs and were following corporate directives. The statistics for sales were posted in the breakroom and it was noted the staff without suitable levels of sales may not be needed.

Follow-Up

Office Depot apparently is investigating the issue, and has stated they do not support the alleged actions, and will take the appropriate steps. With the corporate environment, the extent of the investigation may vary greatly dependent on the number of variables. To ensure this is actually investigated fully, Senator Maria Cantwell (D-WA) has requested the FTC review these claims.

About The Author



Charles Parker, II began coding in the 1980's. Presently CP is an Information Security Architect at a Tier One supplier to the automobile industry. CP is presently completing the PhD (Information Assurance and Security) with completing the dissertation. CP's interests include cryptography, SCADA, and securing communication channels. He has presented at regional InfoSec conferences.

Charles Parker, II can be reached online at charlesparkerii@gmail.com and InfoSecPirate (Twitter).

Stop building higher fences and start searching the grounds

Scott Millis, CTO of Cyber adAPT, argues the case for re-evaluating perimeter security strategies

John Chambers, the man whose hand was on Cisco's tiller for 20 years, is once reported to have said, "There are two types of companies: those that have been hacked, and those who do not know they have been hacked." It has become a truism.

Just about every organization now accepts it is no longer a matter of "if" they suffer a breach, but "when" and, more importantly, how they can isolate and mitigate the threat.

2016 was a record breaking year for reported data breaches, up 40 per cent from 2015ⁱ. In August last year, Yahoo confirmed at least 500 million Yahoo user details had been stolen... in 2014, taking two years for the company to admit it had fallen victim to the largest data breach from a single site in history.

This begs the question: how do you build a security strategy in a world where whatever you do, threats cannot be kept out? The answer lies in taking a new approach. Traditionally, organizations have focussed on their perimeter.

Essentially, they have built big walls to keep out the bad guys. In striving to keep the enterprise safe, these walls have become bigger and more resistant.

But those walls are not impermeable. You can bet your bottom dollar malware and other threats can get past the biggest, best-built barriers surrounding the perimeter of an organization's network.

This is because the way in which attackers approach the perimeter has shifted. Criminals often get in using legitimate usernames and passwords to avoid detection.

These can be gained through phishing, key stroke loggers or even good old fashioned shoulder-surfing.

Of course, there is also the chance of a malicious insider. We all potentially have our own Edward Snowden – although whether he was malicious or not is a point for debate.

This is compounded by technical developments such as virtualization, cloud and mobile. Virtualization makes servers, applications and data both fluid and mobile.

Cloud puts data beyond the traditional confines of a network and mobile means data is pushed out to any number of end points, via a carrier network, often with no more security than a PIN.

These endpoints also have Wi-Fi, Bluetooth and apps which open up huge security holes.

For all these reasons, it is time to stop proverbially staring forlornly along the fence and start searching the grounds. As John Chambers' truism reminds us, the invaders have already breached defences such as firewalls, anti-virus and intrusion detection systems.

At best they are sitting dormant, waiting to pounce. At worst they are stealing, viewing and causing trouble, totally unfettered. In fact, on average an attacker can sit unnoticed on victim's network for 146 daysⁱⁱ.

Clearly, a lot can happen in that time. Information can be extracted, identities forged, cash stolen and infrastructure broken, all of which can spell disaster.

This is why the best defence is not to build a bigger fence, but to analyse network traffic and detect suspicious activities.

This does not mean just checking files to see if they match the profile of known threats, but looking at what traffic is passing over the network and whether it suggests malicious intent.

It means looking for patterns of behaviour that do not look right.

For example, when you or I search for something online, we will probably head for Google. We will do some searching, flick through results, go back, tweak the search terms and generally take a hit and miss approach.

Eventually, we will find what we want and click on the appropriate link. This is a very human process and creates a set of log files that look a certain way when analysed.

The difference between typical malware and a human is obvious in this case, and the traffic and resulting log files should be a warning. Not just that something nasty is on the network, but that nasty thing is starting to do something.

As soon as you know it is doing something – or trying to do something – you can stop it in its tracks. Fast.

This is the approach all organizations should be taking: looking for suspect activity, not suspect files. By taking this high-speed, analytical view of network traffic, you can understand what is good and what is bad, allowing you to pick out anything that got past the perimeter.

The result is the ability to see more attacks, more quickly, and – importantly – reduce false positives.

This is important, because security teams spend so much time checking to see if something really is malicious.

It drains resources and pulls teams away from the more important priorities.

This methodology also allows security teams to focus on malware that really is a threat – not every bit of redundant malware floating around that's inert or inactive. It's a bit like learning to live with slugs in your garden.

You can probably deal with them if they are not doing any damage. But if there are flesh-eating ones, you might want to get some slug bait.

However, understanding what constitutes suspicious activity is no mean feat. It takes a great deal of expertise and understanding to codify and implement. But it is possible. To do so, you need to get inside the head of the attacker and understand their motives and intent.

Broadly speaking, there are only a handful of things that a hacker is trying to do: steal credentials, extract funds, undertake reconnaissance, shut something down (such as critical infrastructure) or embarrass someone.

To achieve any one of these, there are many different tactical pieces of malware, which change and become ever harder to identify over time. But regardless of the malware being used, there is a process that often looks very similar.

If you can understand the intent and the process that goes with it, you can spot suspicious activity that is indicative of the intent and stop the attacker in their tracks. The example of malware connecting directly to an IP address is just one of many.

Organizations need to work with experts to identify these processes and the types of traffic they create. They need to keep up with the cyber criminals and how they operate once they are inside a network.

They need to constantly extend the breadth of detectable behaviour patterns and identify the cause and spread of attacks to power remedial action. Of course, this is a huge investment for an in-house team, which is where security vendors can step in.

In conclusion, while still important, perimeter security is increasingly losing its ability to protect. Building bigger and better walls will stop a proportion of attackers, but it is increasingly expensive with diminishing returns.

The real effort needs to be turned to the grounds within those walls i.e. the network. Doing so will take bravery, but if we do not, organizations run the risk of disaster and security professionals will have lost the battle. And probably their jobs.

Gartner Security & Risk Management Summit 2017

June 12 – 15 / National Harbor, MD
gartner.com/us/securityrisk

Manage Risk. Build Trust. Embrace Change.

Key benefits

- Reinvent your approach to security and risk for the digital age
- Embrace new ways of protecting vital assets without slowing interactions
- Learn how to shift to more adaptive, dynamic, people-centric approaches to security
- Build a trusted, resilient environment for digital business

For more information and to register, visit gartner.com/us/securityrisk. Use promotion code GARTMP4 to save \$300 on the standard registration rate.

“I was impressed with the forward-looking nature of the topics covered at the summit.”

Steve Logan, GTAS Senior Project Manager, Security & Privacy, Vanguard



Jeffrey Wheatman
Director, Gartner Research



Ransomware and the Internet of Things

IoT ransomware is more dangerous than traditional ransomware

Ransomware has become one of the [most serious cyber threats](#) these years. Today, all of us - from home users to corporations and government organizations - are trying to protect ourselves from encryption viruses. However, we still ignore the beginning of the next wave of ransomware attacks aimed at encrypting IoT devices. It can be much more dangerous given the omnipresent and extremely diverse nature of the Internet of Things.

IoT ransomware has already been discussed [online and at security conferences](#), but it was not considered a serious threat at the time. There are some differences that make IoT ransomware more dangerous than the already widespread extortion viruses for desktops and smartphones.

IoT ransomware does not encrypt your data

The well-known and most active crypto viruses like Locky and Cerber lock down important files on infected machines. Their main strength is irreversibility - the victims are forced to either pay for obtaining the decryption key or say goodbye to their files in case there are no backups. It is usually assumed that files and important data have a value expressed in money, and this fact attracts cyber extortionists. IoT devices often do not have any data at all. Some may think that ransomware authors are not interested in attacking IoT devices. It's not actually so.

Instead of only locking some files, IoT viruses may lock and get complete control over many devices and even networks. IoT malware may [stop vehicles](#), disconnect the electricity, even stop production lines. Such programs can do much more harm, and therefore hackers may demand much larger ransom amounts. This increases the attractiveness of the new underground market. One could argue that IoT hacking can be stopped with a simple reboot. However, the incentive to pay extortionists does not result from irreversibility but rather from the volume and character of potential losses which may occur during the time you lose control over the system.

While the Internet of Things expands the possibilities of life-supporting devices like pacemakers or industrial systems such as pumping stations, the financial benefits of blocking IoT infrastructure and the damage from belated response will grow exponentially. Organizations that use the Internet of Things in industrial control systems are the most vulnerable. These include power plants, big automated production lines, etc.

Consumer IoT devices

Attacks on consumer IoT devices, including smart homes and connected cars, are already real. [Researchers have shown](#) how they can gain control of a connected thermostat through the use

of malicious code and set the device to increase the temperature to the maximum, causing the owner to pay a ransom.

Let's imagine you got into a connected car this morning and suddenly there is a message on the screen: "If you pay \$500, I'll let you get to work today." It was impossible several years ago, but due to technological progress, such scenario does not look fantastic anymore.

Furthermore, IoT ransomware may steal important data and personal information, for example, from surveillance cameras connected to the network or from fitness gadgets and then blackmail people, threatening to publish their sensitive information.

Despite the fact that IoT devices often have serious security weaknesses, it is still premature to talk about the imminent ransomware threat for smart homes and connected cars. The wide variety of apps and devices created by thousands of manufacturers complicates extensive malware usage.

The IoT industry is highly fragmented these days. It lacks standardized approaches, common platforms and communication systems. It is tough to carry out mass attacks. Every time a compromise occurs, hackers only target a specific type of devices, which reduces the number of potential victims.

We can conclude that hackers' benefits from attacking consumer IoT devices are currently small. But the situation is likely to change in the future as the Internet of Things is going to deeper penetrate into our homes and offices.

Industrial segment already facing high risks

We see an entirely different picture in the industrial segment of the Internet of Things. Industrial systems are already very attractive for cyber extortionists. This could be any relevant system that may affect the lives of thousands or millions of people and are extremely expensive to operate.

For example, several US hospitals have undergone a series of ransomware attacks recently. Normal workflow of the [Hollywood Presbyterian Hospital](#) was disrupted because of ransomware. Some patients had to be moved to other clinics, and doctors started to keep records the old fashioned way on paper.

If a hospital system is compromised, it puts the health of patients at risk. The likelihood is very high that the hospital will pay upon demand. An attack against [critical infrastructure](#) can be carried out successfully based on similar factors - if lives of people might be put in danger and time is pressing, the owners would often agree to pay up. Power grids and power stations can be another important target for IoT malware. Their important role in the modern world was perfectly illustrated by the [Northeast blackout of 2003](#). It caused \$6 billion in losses within several hours, affecting 55 million people. It wasn't a cyber attack but a software failure. Today, hackers constantly scan the Internet for important and vulnerable networks, so energy companies should be prepared.

How to protect IoT systems from ransomware

Although there is no universal solution, many experts believe that the observance of certain guidelines and methodologies can help organizations and manufacturers better protect their IoT systems from ransomware. One of the important points is the ability to remotely upgrade the firmware of smart devices. Safety is a journey, not a destination, and there are no connected devices that can stay safe forever. Therefore, a firmware update should be a very simple, effective and safe process. The latter is particularly important since insecure update channels can become portals for the infection to come in. There are time-tested measures to eliminate this malware entry point, such as blocking the processor and firmware, as well as encrypting communication channels between devices.

A reliable authentication mechanism poses another important protection measure. You may encounter situations these days when devices are connected to the Internet without any authentication at all. This paves the way for [spoofing](#). If lack of authentication becomes a mass phenomenon, it will be possible to disable millions of devices. Spoofing is particularly dangerous when a server with millions of connected machines is infected.

To make intruders' life much harder it is necessary to introduce reliable security certificate life-cycle management and standardize the code base of security systems. This will help reduce the number of attack vectors.

Of course, securing the Internet of Things remains an arduous task as the industry is only groping its way. Currently, online criminals are only beginning to weigh the risks and assess the opportunities and potential profitability of the new market. Meanwhile, manufacturers and users are not too concerned about the possible threat. Perhaps this will change quickly after the first successful incidents of rogue monetization of IoT vulnerabilities. Hopefully, we will have time to prepare.

About the Author



David Balaban is a computer security researcher with over 15 years of experience in malware analysis and antivirus software evaluation. David runs the Privacy-PC.com project which presents expert opinions on the contemporary information security matters, including social engineering, penetration testing, threat intelligence, online privacy and white hat hacking. As part of his work at Privacy-PC, Mr. Balaban has interviewed such security celebrities as Dave Kennedy, Jay Jacobs and Robert David Steele to get firsthand perspectives on hot InfoSec issues. David has a strong malware troubleshooting background, with the recent focus on ransomware countermeasures.

ALL ACTIVE MILITARY & GOVERNMENT EMPLOYEES CAN ATTEND FOR ONLY \$25!

3RD ANNUAL CYBER SECURITY FOR DEFENSE

Protecting Our Nation Against Faceless Enemies

NEW SPEAKERS FOR 2017:



SHERRILL NICELY
Chief Information
Security Officer
Central Intelligence
Agency



STEVEN SHIRLEY
Executive Director,
Defense Cyber Crime
Center
Air Force Office of
Investigations



TONYA UGORETZ
Director, Cyber
Threat Intelligence
Integration Center
Office of the
Director of National
Intelligence



TRENT TEYEMA
Section Chief (SES)
Federal Bureau of
Investigation



**CHRISTIAN
LIFLANDER**
Head of the Cyber
Defence Section
NATO



200+
Attendees



20+
Defense Cyber
Security Speakers



10+
Hours Of
Networking

Expert Presentations
From The Military,
Government, Law
Enforcement, And
International Military
& Government

Receive An Exclusive 20% Discount Off Standard Rates

Use Code: 'CyberDefenseMagazine_20'

www.CyberSecurityForDefense.icpc.com

The Myth Behind Frequent Password Changes

Are they good practice or counterproductive?

By Sarosh Petkar, BS/MS Student, Computing Security - RIT

INTRODUCTION

Mandatory password changes are an age-old security practice within numerous organizations. This practice is described as a mechanism to lock out unauthorized users who may have managed to social engineer the user's password. Most office employees have to deal with this, as their office system administrators keep sending annoying reminders to keep changing passwords periodically. Is this a requirement or practice that has been so ingrained that its acceptance is no longer questioned?

As per widespread opinion, periodic password changes are theoretically a good idea as they ensure the security of a user's password. This opinion is based on the belief system that constantly changing passwords would prove to be a herculean task for nefarious actors to figure them out. But in reality these regular password changes tend to be an inconvenience to users, and at the same time alters user behavior to choose weak passwords, as they know they will have to change it in a few months time.

BACKGROUND

A recent University of North Carolina (UNC) research, outlined by FTC Chief Technologist Lorrie Cranor agrees that doing periodic password changes can be counterproductive, as it encourages poor password selection by the users. The study suggests that when people are forced to change their passwords periodically, they tend not to put much thought behind it. Users are inclined to choose passwords that are simple to compensate for the frequent changes required of them.

According to the UNC study, people have a habit of choosing passwords that follow a predictable pattern, which is technically called 'transformations.' These transformations are characterized as the addition of a number, deletion of a special character or switching the order of the numbers. These researchers obtained cryptographic hashes (of all passwords) to around 10,000 expired accounts whose users had been required to change their passwords every trimester.

By studying the data, the researchers identified common techniques that users deploy when changing their passwords. For instance, a password like *mrcoolguy@1* (without the quotations) after alteration ended up being *Mrcoolguy@1* on the second change and so on. Further, it may

be changed to either *mrcoolguy@11* or *mrcoolguy@2* and so on. These iterations do not aid in increasing the complexity of the password significantly.

Additional research at Carleton University suggests that if an attacker is already aware of your password, then it is highly unlikely that he will be warded off by a simple password change. In some cases an attacker might already have installed some malicious keylogger to grab all future passwords. So changing passwords in this scenario would be an exercise in futility. Finally, over the past few years, organizations such as the National Institute of Standards and Technology (NIST) in the US and the National Technical Authority for Information Assurance (CESG) in the UK have concluded that mandated password changes are often ineffective or counterproductive.

RECOMMENDATION

So the question remains, how often does a password need to be changed? Unfortunately, there is no definitive answer. Regularly changing your password is essential if you use the same password everywhere and you have a strong suspicion to believe that your password has been stolen. This should be done on all accounts that use the same password. Rather than changing the single password regularly, a wise choice would be to use complex unique passwords for all applications.

However, remembering unique passwords for all the applications is quite impossible - hence a password vault like 1Password or LastPass must be used. These third-party applications come with their own set of issues, but at this point it is a case of making a conscious risk acceptance decision to eliminate the risks inherent in password reuse.

Which begs the question, what are good practices to use when creating a complex password? Well known, security and privacy expert Bruce Schneier recommends the following:

1. Never reuse a password you care about. Even if you choose a secure password, the site it is for could leak it because of its own incompetence.
2. Don't bother updating your password regularly. Sites that require 90-day -- or whatever -- password upgrades do more harm than good. Unless you think your password might be compromised, don't change it.
3. Beware the 'secret question.' You don't want a backup system for when you forget your password to be easier to break than your password.
4. Finally, if a site offers two-factor authentication, seriously consider using it. It is almost certainly a security improvement.

CONCLUSION

In conclusion, the first step towards password security is to assess the risks and benefits to your organization. Next, consider deploying alternative methods towards increasing security. Most experts agree that mandating password expirations is an inconvenience to end-users without

any benefit to security and may even create a less secure environment for the previously stated reasons.

What should be done?

Organizations must encourage users to make an effort to create strong passwords that they will be able to use for a longer period. This policy in combination with periodic security awareness training, well chosen salts, and limited login attempts will help to increase password level security.

However, the gold standard that companies should establish – especially if the enterprise maintains sensitive data is to implement either biometrics or multi-factor authentication.

For example, there are some token generators that provide “three-factor” authentication (username, password and token code). Some systems might even require you to answer some pre-negotiated questions or select a specific photo from a group of images. These add an extra layer of security to the user accounts.

I believe it is crucial to find the balance between convenience and keeping corporate information secure. In that respect, multi-factor authentication seems to be the best approach moving forward. Experts like to rant about how the end-users are the weakest component of enterprise security. But, with MFA becoming as ubiquitous as tweeting for millennials, this mechanism is already at the user’s fingertips.

Recently, even Apple has sent out friendly reminders to encourage its users to enable 2FA to provide an extra layer of security for its iCloud data as well as for all other devices. Thus, on comparing the convenience of the standard username and passwords with multi-factor authentication methods, it looks like the latter seems to prevail.

Ergo, organizations should ruminate about the pros and cons of mandatory password changes and then consider making calculated user-centered changes to their password policies instead of forcing its employees to constantly keep changing their login passwords.

About The Author



Sarosh Petkar is a BS/MS student of the RIT Computing Security department. He is on his way to Mountain View, CA for a summer internship with Veritas and has previously worked with Covermymeds in Columbus, OH. His interests include reverse engineering, network security and cryptography.

Sarosh Petkar can be reached online at sap6224@g.rit.edu



INTERPOL World 2017 Congress

Register now before 31 May 2017 to enjoy early bird rates



Shedding light on the "Dark side" –
Cyberspace and the future of security



Prevention – Getting smarter,
faster and more precise



Identity management and
detection in a borderless world.

World Economic Forum (WEF) addresses cybercrime

WEF's 'Recommendations for Public-Private Partnership against Cybercrime' highlighted the need for information-sharing and cooperation platforms between businesses and law enforcement, with the INTERPOL Global Complex for Innovation (IGCI) in Singapore recognized as such a model.

A workshop dedicated to the implementation of the initiative's recommendations will be held in IGCI on 3 July, followed by a Dialogue on cybercrime on 4 July at INTERPOL World 2017 Congress.



INTERPOL World Dialogue, 4 July 2017
moderated by

Dr Jean-Luc Vax
Head of Public Security Policy and Security Affairs
Member of the Executive Committee
World Economic Forum



SPEAKERS INCLUDE



Arthur Holland Michel
Co-Director
Center for the Study of the
Drone, Bard College



Christian Karam
Director and
Global Head of
Cyber Threat Intelligence
UBS AG



Dr John Coyne
Head of Border Security
Program
Australian Strategic Policy
Institute



**Commander
Jorge R. Rodriguez**
Commander
Los Angeles Police Department



Michael Hershman
Group CEO
International Centre for
Sport Security (ICSS)



Rob Leslie
Chief Executive Officer
Sedicii Innovations Limited

INTERPOL World 2017 Exhibition

EXHIBITION HIGHLIGHTS



PUBLIC SAFETY
TECHNOLOGIES



BIOMETRICS



IDENTITY
SOLUTIONS



FORENSICS AND
INVESTIGATIONS



CYBERCRIME

Register at www.interpol-world.com or contact us at visitor@interpol-world.com

EVENT OWNER



SUPPORTED BY



INDUSTRY INSIGHTS BY



HELD IN



MANAGED BY



The Fatal Danger Lurking in Today's Fortune 500

By Tatu Ylonen, founder and SSH Fellow, SSH Communications Security

It takes a special combination of leaders, ideas and processes to become a Fortune 500 company. By the time an enterprise has reached this status, it has gained significant resources and name recognition, fueled by innovative ideas and the drive to succeed. But if the enterprise does not address a critical danger lurking in its information systems, it could quickly become a Fortune 0.

Access Gone Wild

Enterprises carefully control access to servers and disaster recovery data centers. Behind the traditional applications, servers are managed by system administrators and various automated tools.

The automated systems need credentials to gain access to other systems in order for daily communications and operations to function, and they usually use what is called SSH keys, which are also used by system administrators and developers to do their work internally, in order to log in from their workstation to access servers without having to type their password all the time.

Roughly 90 percent of the SSH keys are unused in the average enterprise. That means there is privileged access to critical systems and data that has never been terminated – violating policies, regulations and laws. It is almost as if employees' user accounts were never removed when they left, and they had the capability to create new accounts for anyone they like.

Even more worrisome is the fact that about 10 percent of the SSH keys grant root access (highest-level administrative access).

Such keys are used to make backups, install patches, manage configurations and implement emergency response procedures, often using automated tools.

To provide the magnitude of the usage of SSH keys, in some enterprises there are more than 5 million automated daily logins using SSH keys – resulting in more than 2 billion logins per year.

The SSH Stealth Attack

A cybercriminal begins an attack by gaining access to a company computer and then steals passwords or other credentials to gain access to a set of servers. This often involves malware.

Once on a server, the attacker obtains elevated privileges using locally exploitable vulnerabilities to read private SSH keys from the server. Many of these keys grant unrestricted access to other servers and systems.

The attacker uses these keys to gain access to those other servers and repeats the process to move undetected within the enterprise.

It is likely that the attack can easily spread to nearly all data centers in the enterprise, given the high number of keys (10-200 per server on average in most enterprises).

Some companies with more than 100,000 keys are granting access from low-security test and development into production servers alone. Key-based access between data centers is almost always present.

Usually, there are also many SSH keys granting access from individual user accounts to privileged service accounts, bypassing systems that were supposed to monitor privileged access.

Cybercriminals use sophisticated means to avoid detection. They can monitor the server for days or weeks to see which SSH keys are actually used with which servers and then piggyback on legitimate connections to move undetected.

Bringing the Fortune 500 to Its Knees

At this point, the digital interloper may confuse the system or destroy it outright. They can modify database records in subtle ways, corrupt backups or render every penetrated server, storage device and router inoperable.

For example, the attacker can reprogram the firmware on routers and switches, install malware into disk drive firmware, network adapter firmware or bios firmware, as well as wipe any data on the affected servers and storage systems, including any penetrated backup systems and disaster recovery systems.

This would be a crippling blow for a Fortune 500. IT teams would need weeks or months to rebuild and reinstall its systems, and it would likely lose a good number of recent transactions.

How many hours, days or weeks can a typical Fortune 500 be down before the reputation damage is irreparable?

The damage to shareholders could easily exceed \$30 billion, given the extent of the damage and the inability to operate or even communicate.

These days, there are multiple possible reasons for launching such an attack. Perhaps a nation-state in a cyberwar might conduct such activity to as many enterprises as possible, even attacking multiple enterprises simultaneously.

Perhaps a terrorist organization wants to cause chaos. Perhaps a hacktivist wants to teach investors not to put money in “unethical” enterprises. Perhaps a criminal organization wants to extract ransom.

For many others, the point would be to extract information, a breach committed to gain competitive intelligence. In such cases, privacy and regulatory issues would be of paramount concern.

Steps to Security

Essentially, this is an administrative problem. No quick fix is available. Enterprise operations totally depend on automation made possible by SSH keys. Enterprises must establish proper management of automated access just as they manage passwords. They must also sort out the legacy mess.

The sooner this is accomplished, the sooner the enterprise can rest easier. The first step is to establish a controlled provisioning process. Unused and policy-violating SSH keys must be destroyed, and application teams need to justify with sign-off on any remaining keys that provide access to the information systems they are responsible for managing.

Tools are available today to assist with this process, as the problem is typically too large to tackle manually.

As a final step, carefully review SSH key-based access into backup systems and disaster recovery data centers to close the loop. Fortune 500s and other enterprises that take these steps have taken back control of a situation that could otherwise devastate them and their shareholders.

About the Author



Tatu Ylonen is the founder and SSH Fellow of SSH Communications Security and the creator of the SSH protocol and the founder of [SSH Communications Security](https://www.ssh.com/). He is an experienced entrepreneur, manager and engineer. He still keeps up to date with technology and loves the technical side and inventing new technology.

He participates in product architecture design and occasionally writes code when he has time or when he thinks that's where he can bring the most value.

His primary current interests relate to broader cybersecurity priorities and how to design systems to be more secure. He understands both the big picture and the deep technical issues. He also wants to solve the massive gap in identity and access management in relation to SSH key based credentials.

Tatu can be reached online at @tjssh and at the company website: <https://www.ssh.com/>.

The Why and How of GDPR (General Data Protection Regulation) for your business

Introduction

The General Data Protection Regulation (GDPR) is an act which comes into effect from 25th May 2018, consists of 173 recitals enforced by 99 articles and is applicable

- Across the EU, when the data processing occurs within the EU
- To the goods or services within the EU
- To the personal details of the EU individuals
- For monitoring the behavior of EU citizens (when such behavior occurs within EU) and
- Overrides the Safe harbor provisions earlier used to govern the data transfer between US and Europe

General Data Protection Regulation (GDPR)

GDPR harmonizes the various data protection laws across the EU and is applicable to both the Data “controllers” and data “processors” where

- a) “Data Controller” is the business entity that determines the purposes and means of processing the personal data
- b) “Data Processor” is the entity that processes the personal data on behalf of the data controller

Personal Data

In the context of GDPR, the term “Personal Data” refers to the -

- Names,
- Residential Addresses,
- Business contact information, Trustees, Officers and Shareholders,
- Business qualifications, Licenses and registrations,
- Suppliers, Vendors and Sub contractors,
- Legal agreements,
- Insurance policy numbers,
- Medical information,
- Vehicle registration numbers and related offences,
- Payroll, Financial details (taxation, credit worthiness), Pension related details,
- Enrolled benefits and beneficiary details,
- Social security number,
- Employment related – such as Company name and Designation,
- Capital and Property related details,

- Food and marketing preferences,
- Travel related profile (Frequent Flier details and preferences),
- Insurance agencies and intermediaries, Health advisors, Financial and Legal representatives,
- Back ground checks and Recruitment history, Performance related records,
- Employee Share Purchase Scheme,
- Family and Relatives details,
- Religious, Philosophical beliefs,
- Racial or ethnic origin, Political opinions,
and any other sensitive personal data which uniquely identify an individual (can be person or business)

And such “Personal Data” resides in any of the following formats -

1. Saved or recorded documents on computer systems,
2. Email,
3. Sound recordings,
4. SMS, or multimedia messages,
5. Encrypted tokens, Passwords,
6. Visual images,
7. Manual data including but not confined to correspondence

Key features of GDPR

1. It strictly imposes 72 hours’ time limit to report the data breach to your data protection authority
2. It must be complied with from May 2018 onwards
3. It imposes hefty fines for non-compliance (refer Appendix A)
4. It puts responsibility on the Data Processor and Data Controller to demonstrate how they fulfill the compliance requirements
5. Covers everyone who collects and/or processes the personal data

Data Protection - Principles

The following data protection principles form the foundation of the key features of GDPR -

<u>Principle</u>	<u>Description</u>
Purpose Limitation	That the collected data shall be only used for specified, explicit and legitimate purposes and not processed in any manner that violates the declared purpose(s)

Lawfulness, Fairness and Transparency	That the collected data shall be transmitted and processed in a lawful, fair and transparent manner such that the data processor and data controller are clear on what is the type of data and what is the intended purpose for using it
Accuracy	That the collected data shall be kept up to date
Data minimization	That the collected data shall be relevant and limited to what is necessary for fulfilling the declared purpose(s) only
Storage limitation	That the collected data shall be not retained and/or stored beyond when it has fulfilled its declared purpose(s)
Confidentiality and Integrity	That the collected data shall be processed in a manner that ensures appropriate security of the personal data
Accountability	That the collected data shall be used to enable the data controller demonstrate compliance with these data protection principles and maintain the records of appropriate processing activities

Exceptions to GDPR

GDPR is not applicable in the following circumstances -

1. When the information is processed purely for personal or in-house purposes
2. When the information is processed by competent authorities (such as involving criminal investigations)
3. For companies with <250 employees, unless the processing of the personal data poses high risk, there is no need to designate a data protection officer (DPO)
4. When data processing is a subsidiary activity so it's not compulsory to maintain documentation related with data processing operations

GDPR Terms

- “Personal data”, special categories of data, process/processing, controller, processor, data subject and supervisory authority have the same meaning as specified in the Data Protection Directive 95/46/EC of the European Parliament on the protection of individuals, about the processing of personal data and on the free movement of such data
- “Data exporter “controls the transferring of the personal data
- “Data importer “is the entity which agrees to receive the personal data from the data exporter and processes it while ensuring adequate protection (within the meaning of Article 25(1) of Directive 95/46/EC) on behalf of the data controller
- “Sub Processor” is the Data Processor which is engaged by the data importer and receives the personal data exclusively to perform the processing activities on behalf of the data exporter
- “Applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals; and their right to privacy in terms of the processing of their personal data
- “Data subject” is the person whose personal data is transferred or the people who receive the benefit of such data processing services
- “Technical and organizational security measures” are those which are aimed to protect the personal data against unlawful destruction or accidental loss, alteration, unauthorized disclosure and/or access, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Entity Wise - Obligations

Now let us understand the obligations of the various involved entities.

The **Data Exporter** is obligated to ensure that

- It can demonstrate compliance with the Data Protection principles mentioned above
- The processing and transferring of the personal data is done in accordance with the relevant and applicable data protection laws and without violating the conditions set forth by the relevant authorities of member state where the data exporter is established

- It has suitably instructed the data importer to process the personal data only on behalf of the data exporter and in accordance with the applicable data protection laws and contractual clauses
- It has taken guarantees from the data importer about providing at least the following (contractually agreed) technical and organizational standards and measures -
 - Acceptable Use
 - Access Management
 - Anti-Malware
 - Data Management and Data Protection
 - End User Computing
 - Application Security
 - Licensing
 - IT Performance, Risk and Compliance
 - Logging and Monitoring
 - Mobile Devices Security
 - Cloud computing and Storage
 - Patching
 - Remote Access Security
 - Third party Management
 - Vulnerability Management and Penetration Testing
 - Web Application Security Testing

to be able to ensure reasonable compliance which is –

- Appropriate to the risks posed by such data processing and
- Is commensurate with the sensitivity of the personal data being protected and
- Keeps in mind the overall cost of implementation
- (In the event of sub-processing) The data processing activities are done while maintaining the same level of protection for the personal data and safeguarding the rights of data subjects
- It securely maintains a list of sub-processing agreements as notified by the data importer, reviews/updates this list at least once a year and makes this list available to the data exporter's data protection supervisory authority
- It conducts an impact assessment when a new processing activity poses high degree of risk for the data subjects' information
- It provides the requested information to the data subjects within max. one month of receiving such service access request from the data subjects; Along with providing a summary description of the security measures and the contractual clauses which govern the processing services (commercial details can be removed)

The **Data Importer** is obligated to ensure that

- It has implemented the information security controls such as policies, practices, procedures and organizational structures to adequately protect the confidentiality, integrity and availability of its own data and the data of its data exporter
- The IT, technology and outsourcing services which it provides to the data exporter are adequately secure and reliable
- It processes the personal data only on behalf of the data exporter and in compliance with its instructions and contractual clauses
- If, for any reason, it cannot provide such promised levels of compliance, it shall promptly inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or even terminate the service agreement (contract)
- It shall promptly inform about the legislation related changes to the data exporter as soon as it becomes aware, in which case the data exporter is entitled to suspend the transfer of data and/or even terminate the service agreement (contract)
- It can provide at least the following (contractually agreed) technical and organizational standards and measures -
 - Acceptable Use
 - Access Management
 - Anti-Malware
 - Data Management and Data Protection
 - End User Computing
 - Application Security
 - Licensing
 - IT Performance, Risk and Compliance
 - Logging and Monitoring
 - Mobile Devices Security
 - Cloud computing and Storage
 - Patching
 - Remote Access Security
 - Third party Management
 - Vulnerability Management and Penetration Testing
 - Web Application Security Testing

to be able to provide reasonable assurance to the data exporter

- It shall securely maintain the records of its data processing activities

- It shall properly abide by the advice of the supervisory authority regarding the processing and/or transfer of the personal data
- It shall promptly notify the data exporter as and when
 - Any legally binding request for disclosing the personal data comes from a law enforcement authority
 - Any request is received directly from the data subjects
- It shall promptly and properly respond to all the inquiries from the data exporter relating to how it processes the personal data
- It evaluates the risks inherent in the data processing and timely implements measures to mitigate those risks by taking reasonable actions
- Upon request of the data exporter and/or the relevant supervisory authority, subjects its data processing activities and facilities for auditing the deployed security controls, standards and measures, as per the contractual clauses;

Note: Such audit can either be carried out by the data exporter or by an inspection body selected by the data exporter. Such an inspection body

- a) *Comprises of independent members having the required professional qualifications and bound by the duty of confidentiality*
- b) *has been established in agreement with the supervisory authority*

- It has duly informed and taken the prior written consent of the data exporter, before engaging any sub-processor/sub-contractor for doing its operations on behalf of the data exporter
- It promptly sends a copy of the sub-processor/sub-contractor agreement to the data exporter, ensuring that such agreement imposes the same obligations on the sub-processor as have been imposed on the data importer
- It promptly informs the data exporter about any legislation - either on itself or on any of its sub-processors - which prevents the data exported from auditing either the data importer and/or its sub-processors

The **Sub-Processor** is obligated to

- Fulfil its data protection obligations as per the written service agreement (contract) with the data importer
- Abide by the provisions relating to the data protection aspects mentioned in the service agreement (contract) and as governed by the law of the Member State in which the data exporter is established
- Be fully liable to the data exporter for delivering its obligations as per the written service agreement (contract)

Note: Such liability of the sub-processor is limited to its own processing operations under the service agreement (contract) clauses.

- Allow its data-processing facilities to be audited for the deployed security controls, standards and measures, when requested by the data exporter and/or the relevant supervisory authority

Termination of Contract/Completion of Work

Upon completion or termination of the data-processing related services, the data importer and the sub-processor are mandated to -

- a) Return all the personal data transferred to them, including the copies, if any, to the data exporter or
- b) Destroy all such personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying such personal data. In that case, the data importer must guarantee the confidentiality of the personal data and not actively use it any further

Transitioning to GDPR

Now that we have clarity on what is GDPR, let us consider a few practical steps which can enable a company to transition to and comply with the GDPR -

1. Review and reword the contracts around the Model Clauses which provide a standard framework
2. Thoroughly review the binding contractual rules and get approval of your EU data protection agency
3. Enlist your information assets, products and services
4. Assess the security of your data processing activities by performing a gap analysis to understand and refine the scope of compliance
5. Create flow diagrams showing the data processes
6. Conduct data protection impact assessments (DPIAs) by adopting a risk based approach to identify the high-risk activities first
7. Get clarity on how to manage the data subject access requests while keeping in mind the obligations; Define the mechanisms how you shall serve and fulfill such access requests and the associated data transfers
8. Refine and/or establish the legal basis (e.g. contractual clauses, legitimate interest of the data subjects) for retaining the personal data, if applicable
9. Define the incident management related aspects
10. Identify the operational controls, standards and measures
11. Refine the processes for tracking and maintaining the audit trails, logs and records

Appendix A

DPRR PENALTIES TABLE

Article #	Fines	Notes
Article 23: Data protection by design and by default	€10M or up to 2%	Reference to state of the art
Article 29: Co-operation with the supervisory authority	€10M or up to 2%	
Article 30: Security of processing	€10M or up to 2%	Reference to state of the art
Article 31: Notification of a personal data breach to the supervisory authority	€10M or up to 2%	Breach and notification
Article 32: Communication of a personal data breach to the data subject	€10M or up to 2%	Communication of breach to data subject
Article 5: Principles relating to personal data processing	€20M or up to 4%	
Article 7: Conditions for consent	€20M or up to 4%	
Article 15: Right of access for the data subject	€20M or up to 4%	
Article 16: Right to rectification	€20M or up to 4%	

(Reference: ISACA)

About the Author



Vineet Aggarwal CBCP, CISSP, CISA, Certified ISO 27001 Lead Auditor, Certified ISO 22301 Lead Auditor is the Senior Consulting Manager at Wipro Ltd. with more than 17 years Information Security experience in Business Continuity Deployment, Cybersecurity Lifecycle Enforcement, Risk Management, Information Security Gaps Assessment, Data Privacy Assessments, Cloud and Mobile Security Assessment, Vendor Evaluation, Industrial Security Controls Assessment, and Information security Compliance Audits across geographies



SECURITY IT SUMMIT

4 July 2017

Hilton London Canary Wharf

Start your planning for 2018 at the **Security IT Summit**.

Meet with the most trusted solution providers, learn from industry thought leaders and connect with peers over the course of the Summit, which is entirely **FREE to attend** for security professionals.

Topics covered include: Access Control • Anti-Virus Browser • Security Data • Theft/Loss • Malware • Mobile Security • Network Security Management • Trojan Detection • UK Cyber Strategy



For more information and to register, please contact **Liz Cowell** on:
01992 374072 or l.cowell@forumevents.co.uk.



@SECIT_SUMMIT #SITSUMMIT

SECURITYITSUMMIT.CO.UK

MEDIA & INDUSTRY PARTNERS:



HOSTED BY:



E-Lenders: Hackers New Favorite Targets

By Alisdair Faulkner, Chief Product Officer, [ThreatMetrix](#)

Over the past few years, online and peer-to-peer lending have emerged as popular financial options.

Industry pioneer Lending Club reported over \$24 billion in loans issued as of 2016, and since 2007, small business e-lender OnDeck has lent more than \$825 million.

Given the proliferation of all things digital, this new online lending trend shows no signs of slowing down, and it's already resulted in greater financial inclusion for unbanked and/or underbanked consumers, as well as an increase in new account creation transactions.

Common Attack Vectors

At the same time, though, the business of online lending is evolving, with rising interest rates, stricter regulations and increasing competition from traditional banks creating pressure on profitability.

Even more troubling for the industry is the growing number of cyberattacks. ThreatMetrix conducted research on actual incidents of cybercrime from July through September 2016 and found new loan application fraud higher than ever before.

Cybercriminals are viewing e-lenders as easier targets than larger, more established banks, which has led to a surge in the buying, trading, augmenting and monetization of stolen identity credentials.

Loan stacking (i.e. when a consumer takes out multiple loans without a lender's knowledge) has emerged as another common attack vector amongst online lending-focused cybercriminals, as hackers can capitalize on time delays inherent in reporting loan agreements to credit bureaus.

Stolen identity credentials and device spoofing techniques allow cybercriminals to bypass even complex application procedures, and bots have proved invaluable for the mass testing of credentials and the infiltration of trusted user accounts.

The Critical Dilemma

The acute challenge for e-lenders is that stolen identity profiles are becoming increasingly indistinguishable from authentic profiles, because they're created using a plethora of stolen data and resemble near-blueprints of the real thing.

It requires significant time and industry expertise -- resources few organizations have -- to systematically peel beneath the layers and pinpoint a spoofed device, cloaked location or anomalous personal credentials that can indicate a hack.

It should no longer come as a surprise, then, that static information stored by online lenders, such as usernames, passwords, security questions or even personal information, is no longer an effective authentication method.

Instead, the only way to truly remain secure -- and also process transactions in a manner expected by today's tech-savvy consumers -- is by analyzing the digital identity of every online user.

Trusted, Digital Identity Data

Individual, digital identities leverage dynamic, shared intelligence pulled from more sources than just the various companies a user transacts with. This is possible via behavioral analytics, which can analyze a user's intricate online footprint and provide a unique way of identifying anomalous and high-risk behavior, and machine learning, which can create a predictive model based on past behavior and transaction data, and produce more accurate and actionable models over time.

In deploying digital identity solutions that establish the trust of each user across all data, devices, location and behavior, and by cross-referencing this data in real-time against worldwide threat intelligence, e-lenders can better combat relentless hackers and ensure reliable security for consumers.

Better yet, by taking a more holistic, crowdsourced approach to building a library of digital identity data, e-lenders can accurately differentiate cybercriminals from genuine customers, before it's too late.

About the Author



Alisdair Faulkner
CHIEF PRODUCTS OFFICER

Alisdair is a technology entrepreneur and brings nearly two decades of industry experience to his role leading product management and strategy for ThreatMetrix. He is a noted industry expert in online fraud, cybercrime, identity theft, information security and networking technology and holds several patents in security, fraud and networking. Prior to ThreatMetrix he was founder and Chief Products Officer at NetPriva (now part of Riverbed).

Three Tips to Avoid Going Phishing

By Travis Rosiek, CTO, Tychon

It's an old trick in the physical world. Getting into a secured building is easiest if an infiltrator can get an authorized person to open the door for them. No need to pick locks or smash windows. Just dress like a workman or hold a big bag of groceries and some unsuspecting person will helpfully hold the door. It's little different in network security these days. With potentially thousands of legitimate users accessing secure networks every day, the new trick is to get one of them to unknowingly crack open the defenses.

The technique used to do this is called phishing, and it's constantly found to be one of the top ways networks get compromised. Sometimes called spear phishing if it's especially targeted, phishing is almost always delivered as an email that either looks to be from inside the company or from a trusted or innocuous source. It invites users to either click on a malicious link, open an infected attachment or to provide some type of security or personal information like their password. Sadly, even among a well-trained workforce, it's surprisingly successful. The best attackers know how to manipulate people, and then use social engineering and research through social media and other sources to up their odds.

In fact, at a recent cyber-terrorism summit in New York, Homeland Security Secretary Jeh Johnson called it out, saying that "The most devastating attacks by the most sophisticated attackers almost always begin with the simple act of spear phishing." But as prolific as they are, phishing attacks are not invincible. With the proper planning and tools, they can be defeated just like any other type of attack.

1) Plan for a Phishing Trip

The best time to defeat a phishing attack is before it begins. It's a great idea to train users to try to make them aware of the dangers, but you can never rely on that. The best attackers can mimic an email from the CEO, or human resources, or even colleagues. You can ask users to report suspected phishing emails – though according to the 2016 Verizon Data Breach Report this is seldom done - so that even if someone clicks on it, others may at least bring it to the attention of IT. But someone will almost always take the bait.

By assuming that some users will eventually fall for a phishing attack, IT teams can plan how they will respond from the perspective of knowing that it will happen, not that it's just a possibility. Security Operations Center (SOC) teams can thus plan how to diagnose and triage an attack by putting tools in place to do things like analyzing who is sending and receiving emails at scale. Incorporate all network security tools into that plan, so that any threat, no matter how initially triggered, can be contained and mitigated.

2) Phishing Post Mortem

Organizations should leverage a next generation email security platform along with a capability that allows for retrospective analysis of phishing emails after an attack. This will allow the ability

to create a repository of captured phishing mails so that the tactics and techniques of the adversary can be learned. Things like who is being targeted by the emails, what personal or confidential information was used for social engineering and what actions the email wanted a user to take can all be used to train SOC teams what to expect in the next wave.

Once a sufficient quantity of phishing emails has been collected, they can be used as a training tool, not so much for users who may be a lost cause, but for the SOC teams who need to respond to the threats phishing enables. The one good thing about phishing attacks is that they leave behind a lot of data, and sometimes actual program code that can be analyzed and defended against in the future – if you have the right tools to capture and study that information.

3) Know Where the Phish are Biting

All that data collected in step two can be used for another valuable purpose: predictive analysis. While you may not be able to train every user to defeat every phishing attack, you can selectively warn certain groups who are being targeted. Perhaps your finance group is being targeted by a phishing email that appears to come from the CFO. Or your human resources employees are being sent malicious email packages from fake prospective new employees. Knowing that can be a huge advantage. Being able to collect and analyze phishing emails can unmask trends and active ongoing campaigns against your organization. In that case, giving a specific warning to targeted employees or groups can be highly successful, and might just stave off your next unexpected phishing trip.

About the Author



Travis Rosiek serves as the Chief Technology Officer (CTO) of Tychon, where he is responsible for product innovation and professional services. With nearly 20 years of experience in the security industry, Travis is a highly accomplished cyber defense leader having led several Commercial and U.S. Government programs. He is known for developing and executing strategic plans to build the technical capacity of a company across product development, quality assurance, technical marketing, professional services, and sales engineering.

Prior to his work with Tychon, Travis held several senior roles with prominent security companies including CloudHASH Security, McAfee, and Defense Information Systems Agency (DISA). He also served as the Federal CTO at FireEye. A proud graduate from West Virginia University, receiving his M.S. in Electrical Engineering and dual B.S. in Computer and Electrical Engineering, Travis is also an ISC2 Certified Information Systems Security Professional (CISSP) and a member of multiple task forces and advisory committees.

Travis can be reached via LinkedIn and at our company website: Tychon.io

Best Practices in Cyber Security for Businesses

Cybersecurity--information technology security--is the practice of protecting computers, applications, data, and networks from illegal access.

From hacking to computer viruses, to phishing emails and calls, efficient cyber security is needed now more than ever; throwing up a simple firewall isn't going to cut it these days.

With the increase in technology, there will always be an increase in viruses and hackers and the only way to protect yourself and your business is to become educated on the best practices of cyber security.

What You Should Be Practicing

Operating a business is definitely no walk in the park and there are so many factors that keep a business running smoothly and successfully. Unfortunately, the actions that are taken to practice efficient cyber security are often left by the wayside and not vigorously enforced, leaving businesses vulnerable to vicious hackers and scammers.

Don't let that happen to your place of work; read through the list below of a few beneficial ways to increase cyber security within a business:

Keep Accurate Logs: It is extremely important to keep a record of all systems and applications that run help in running a business. Ideally, this log should be checked on a weekly basis in order to successfully monitor which applications are at risk of security breaching and which are running smoothly.

The great part about logs of application use is that not only will a business be able to detect a security problem from its early stages, they will also have the ability to keep track of the applications and if they are performing to the standards that are needed. It's an all-in-one security and damage control system.

Train Your Users: Running a successful business is a difficult and timely task and putting together a meeting--on top of all the other ones for that day--that all workers can attend can be just as hard, but when it comes to cyber security, it's a necessity.

A business should be trained to know how to create passwords that are strong and hard to hack, know the difference between a safe and reliable application and one that is questionable, and recognize phishing phone calls or emails--when hackers/scammers make an attempt to trick a worker into giving out a business's information such as credit card numbers, login information, or bank account numbers. There's one less thing to worry about when a business is staffed with trained employees.

Carefully Monitor Your Applications That Have Access to Data: Applications are kind of tricky. They are a much needed tool that businesses use to maintain their organization and productivity in order to run a successful and professional operation, but applications also have the unfortunate ability to jeopardize any important data. In many situations, most applications have access to certain critical data just by being on the same hard drive.

Due to this, many hackers find this to be the golden opportunity to hack into and steal data. For hackers, it is much easier to gain access to data through secure applications rather than a business's firewall. Since applications are a much needed tool, the best thing a business can do is monitor them carefully. McAfee runs a great program--McAfee Application Data Monitor--that provides users with application-layer monitoring that prevents any and all types of threats, such as fraud and data loss.

Whether you invest in a program or hire a professional, this step is crucial for better cyber security.

Create Specific Access Controls: Once you have successfully found a source to monitor any applications that have direct access to important data, it is time to create specific access controls.

This is a necessary step for better cyber security since it will limit the number of users that have access to important data.

This step does take time since it requires those in charge to sit down and come up with a list of workers who are allowed to have access to certain applications and the data it exposes, and then further decide which workers only need the applications that are central to their work.

By taking the time to thoroughly sort through and create specific access controls, a business's data will only become more secure and its risk of getting hacked will significantly decrease.

By practicing the above methods of cyber security, you'll never have to worry if your business will take a big hit from an experienced hacker. Safeguard your business and implement the proper cyber security needed to ward off hackers, viruses, and phishing emails and calls.

About the Author



Tim Green has been designing cutting edge OTT and IPTV solutions since 2005. The [founder and CIO of TikiLIVE](#), Tim has bootstrapped the small company from a concept and turned it into an industry leader in just over 8 years. When he is not designing cool modules for TikiLIVE, he enjoys blue water free dive spear fishing from his front yard in the Florida Keys and throughout the Caribbean.

Tips to Help Boost the Security of Your MySQL Database

By Sujain Thomas, Security of Your MySQL Database, Remote DBA

If you have been kept on database security news, you may have heard of the attacks on MySQL databases.

The attacks used to be common on the likes of CouchDB, Cassandra, MongoDB and ElasticSearch. They are now on MySQL.

When you come to think of it, no platform is safe. It is up to you to keep your database safe. There are a couple of things you should consider doing.

Don't leave any 'open doors'

The key to boosting the security of your MySQL database is to start by minimizing the SQL server exposure. This means you need to cover all the 'doors'.

Only install the required components and avoid running your server using an account that has local Windows administrative privileges.

A domain account will minimize exposure. What's more is that you need to edit all the default settings. If you are not using some of the default settings, disable them.

Hackers target the default settings in their attacks.

Limit who can access the server

When planning the user and service accounts, you have to be mindful of user accountability. This will help prevent the misuse of the privileged accounts.

When you have the option of integrated Windows authentication and the built-in SQL server authentication, go with the integrated Windows authentication.

If you must use the second option, ensure that you have a strong password policy. Avoid the use of shared user accounts for the administrators.

For more security, you must always use the dedicated accounts. If you are still confused about which service to use, consider hiring professional [database services](#).

Plan database ownership as well as data security in advance

The mistake most people make is that of making alterations as they go. When it comes to the security of your database, this is not something you should do.

You have to plan everything in advance.

You need to begin by identifying the needed level of protection as well as encryption for your MySQL database.

This is more so if you will be dealing with sensitive data such as credit card or patient health information.

Making sure that you have all the information on data confidentiality will also help. Assign distinct database owners; this simply means that you should not use the same login for all accounts.

There should also be one similar process for new database requests and approvals.

Patch your SQL servers regularly

For added security, you have to come up with a patch management plan.

Remember that attackers are actively looking for more efficient ways of breaking into IT systems.

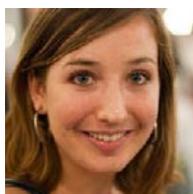
A sound patch management plan will make sure you have implemented the right safety measures to keep malware and viruses out.

Make sure that you have the latest updates at all times.

Improved MySQL database security calls for a thoughtful policy. You have to be proactive in all your actions. The mistake you can make is that of assuming that your servers are impenetrable.

It is wise to always keep checking the soundness of your databases and make sure you implement new security measures as soon as they are available to you.

About the Author



Sujain Thomas is a DBA expert offering database services in California.

She takes pride in helping her clients secure their databases and also sharing information on database security.

The Electric Grid as Our Manager

Lessons from a Recent Issue

by Charles Parker, II

Recently a substantial wind storm blew through the lower peninsula of Michigan. There were wind bursts of, at times, of over 60 miles per hour with sustained winds of 40 mph.

This removed the opportunity for people to use electricity for anywhere of 36 hours to sever days.

The immediate effect for certain parties located in the rather broad brush stroke of the storm happened to be rather drastic.

If parties had generators in place, the effect was significant but not drastic, such as not operating all the equipment or every other of their set of lights. Without a generator, the business imply shuts down for a few days, to the owner and management's detriment.

The effect of this in the latter case tends to vary greatly, dependent on the industry. With a restaurant, there is food to take into consideration. In the cases of a manufacturer, revenue and timing schedules would be definitely affected.

There may be a lag time for a plant to begin manufacturing when shut down for an indeterminate amount of time.

This unfortunate set of events sheds a rather bright light on two aspects within the utility industry. The utilities tend to be rather insecure and presents vulnerabilities.

As an example, in 2016 a waste water treatment plant in Lansing, MI had the pleasure and opportunity of being targeted and a victim of ransomware.

The utility eventually paid the fee for the decrypt key.

Instead of the power outage being caused by a rather substantial storm, this could have easily been the result of an attack on the enterprise, ICS, and/or SCADA.

The latest DDoS attacks show the level of devastation that could occur without a mass amount of effort.

These systems, especially at the utilities, need to be secured appropriately to avoid these issues. In this case of the potential attack, the electricity could be out for several days or longer, not simply 36 hours.

Any equipment damaged during one of these attacks would incur substantial delays.

The equipment utilized at the utilities is rather specialized and not sold at the local hardware store.

Certain pieces of equipment may take weeks or longer to manufacture and ship to a facility.

From the energy recipients view, this issue highlights the need for disaster recovery plans (DRP) and back-up plans.

These both need to be in place, tested, and updated as needed per the environment and as results of the tests. If the business model needs change, these plans likewise need to be updated so that these match the business needs.

These tests may plan for the worst case scenario, however not every aspect would be covered with these table top exercises talking through potential issues. There are always areas that are not fully thought through.

To best test these, the actual issue should be physically introduced. This would work to bring out the other issues not thought through.

The widespread effects of the storm provide an opportunity to think through what may happen to the localized commercial and consumer's utility customers when there is an issue.

Planning with a DR plan and BIA is pertinent and relevant to mitigate the potential effects from attacks or malware. A low level of effect for the utility from the mitigants being applied is important to the clientele and utility.

About The Author

Charles Parker, II began coding in the 1980's. Presently CP is an Information Security Architect at a Tier One supplier to the automobile industry. CP is presently completing the PhD (Information Assurance and Security) in the dissertation stage at Capella University. CP also is an adjunct faculty at Thomas Edison State University. CP's interests include cryptography, SCADA, and NFC. He has presented at regional InfoSec conferences.

Charles Parker, II may be reached at charlesparkerii@protonmail.com and InfoSecPirate (Twitter).

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>



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-intrusive customer experience.

KEY FEATURES

 Cloaking Technology <small>(patents-pending)</small>	 Dynamic Port Management <small>(patents-pending)</small>	 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

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)**

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:

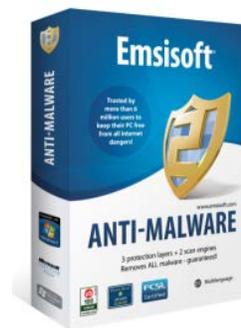
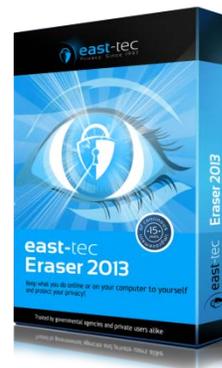
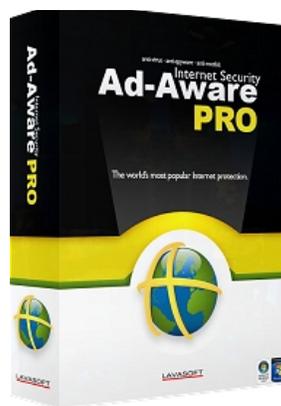
<http://www.naisg.org/techtips.asp>

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 April 2017

Sample Sponsors:



Monitor Mobile Devices
Remotely From Your
Computer



SECURE THE CLOUD. TRUST THE CLOUD.



NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION



CENTER FOR
INTERNET SECURITY

Software Developer's
new ideas & solutions for professional programmers JOURNAL



the power of knowing



SnoopWall
RECLAIM YOUR PRIVACY™



MAKE IT SECURE



BLACK BOX WAN Encryption



June 5
DC Metro
Sept. 18
New York City



18-20 JUNE 2014 - ARLINGTON, VA



See How RSA Security Analytics
Detected Heartbleed
Watch video >>



January 26-27, 2015 New York



March 23-25, 2015 | Orlando, FL



January 21-22, 2015 | Calgary, AB



THE EVENT FOR THE CYBER INDUSTRY



London, 5th February
20% discount (CYSENCDM)



June 14 - 16, 2015 • Charlotte, NC



13-14 April 2015
etc venues 155 Bishopsgate, London

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

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only \$199

Five Year Commitment starting at only \$499

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

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS



Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for April 2017

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...



FalseGuide malware victim count jumps to 2 million

<http://www.zdnet.com/article/falseguide-malware-victim-count-jumps-to-2-million/>

New Strain of Linux Malware Could Get Serious

<http://www.linuxinsider.com/story/84481.html>

Popular Antivirus Flags Windows As Malware And Facebook As Phishing Site By Mistake

<https://fossbytes.com/webroot-antivirus-flags-windows-malware-facebook-phishing-site/>

Hackers uncork experimental Linux-targeting malware

https://www.theregister.co.uk/2017/04/25/linux_malware/

US ISP Goes Down as Two Malware Families Go to War Over Its Modems

<https://www.bleepingcomputer.com/news/security/us-isp-goes-down-as-two-malware-families-go-to-war-over-its-modems/>

Close to 9,000 servers across Asean infected with malware

<http://www.zdnet.com/article/close-to-9000-servers-across-asean-infected-with-malware/>

A Security Researcher Created a Tool to Test for NSA's DoublePulsar Malware

<https://themerkle.com/a-security-researcher-created-a-tool-to-test-for-nsas-doublepulsar-malware/>

A Closer Look at CIA-Linked Malware as Search for Rogue Insider Begins

<http://www.darkreading.com/attacks-breaches/a-closer-look-at-cia-linked-malware-as-search-for-rookie-insider-begins/d/d-id/1328710>

Point-of-Sale Malware Steals Driver's License Information

<https://www.bleepingcomputer.com/news/security/point-of-sale-malware-steals-drivers-license-information/>

A London Police Officer Bought Malware That Can Intercept Calls, Steal Emails, And More

https://motherboard.vice.com/en_us/article/london-police-officer-bought-malware-that-can-intercept-calls-steal-emails-more

HARD TARGET: FILELESS MALWARE

<https://threatpost.com/hard-target-fileless-malware/125054/>

Internet of Things malware Hajime is creating a botnet from 300,000 devices

<http://www.digitaltrends.com/home/hajime-iot-botnet/>

Chinese, Russian Cyber Groups Research Shadow Brokers Malware

<http://www.darkreading.com/vulnerabilities---threats/chinese-russian-cyber-groups-research-shadow-brokers-malware/d/d-id/1328724>

Fake Delta Airlines Receipt Packs Malware

<http://www.darkreading.com/attacks-breaches/fake-delta-airlines-receipt-packs-malware-/d/d-id/1328692>

Australian government plan to force ISPs to block malware

<http://www.computing.co.uk/ctg/news/3008981/australian-government-plan-to-force-isps-to-block-malware>

SAC the security awareness COMPANY

Size Doesn't Matter!

Whether you have 50 or 5000 employees, we have a training package perfect for you! Substitutions + additions are welcome. To see all of our available packages, visit our website!

Package SAT-100A Price: \$795* per year

Choose from one of our packages or design your own. Mix & match from our extensive inventory. Anything you want is possible.

- 12 Monthly Newsletters
- 6 Pieces of Poster Art
- More than 100 pieces of Poster Art
- 12+ Mini Courses and 7 Compliance Modules
- 5 Fundamental Security Awareness Courses
- 30+ Security Express Videos
- 12 Episodes of Mulberry: A Security Awareness Sitcom
- 2 Short Security Awareness Films
- 1 year subscription to Security Awareness News

*Unlimited Internal Licenses for the specified number of users per year. Courses are hosted on your SCORM LMS or Intranet Server. Videos are hosted on your Intranet. Posters may be used electronically or printed in any quantity at any size. **UPGRADES: (1) Brand materials with your logo, name, colors and incident response. (2) We host on our LMS, you administer. (3) Add users. (4) Custom awareness programs.

www.TheSecurityAwarenessCompany.com Call Us to Discuss Your Training Options! +1.727.393.6600 twitter.com/SecAwareCo

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Copyright (C) 2016, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. 848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com
Cyber Warnings Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. Cyber Defense Magazine, CDM, Cyber Warnings, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2016, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

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

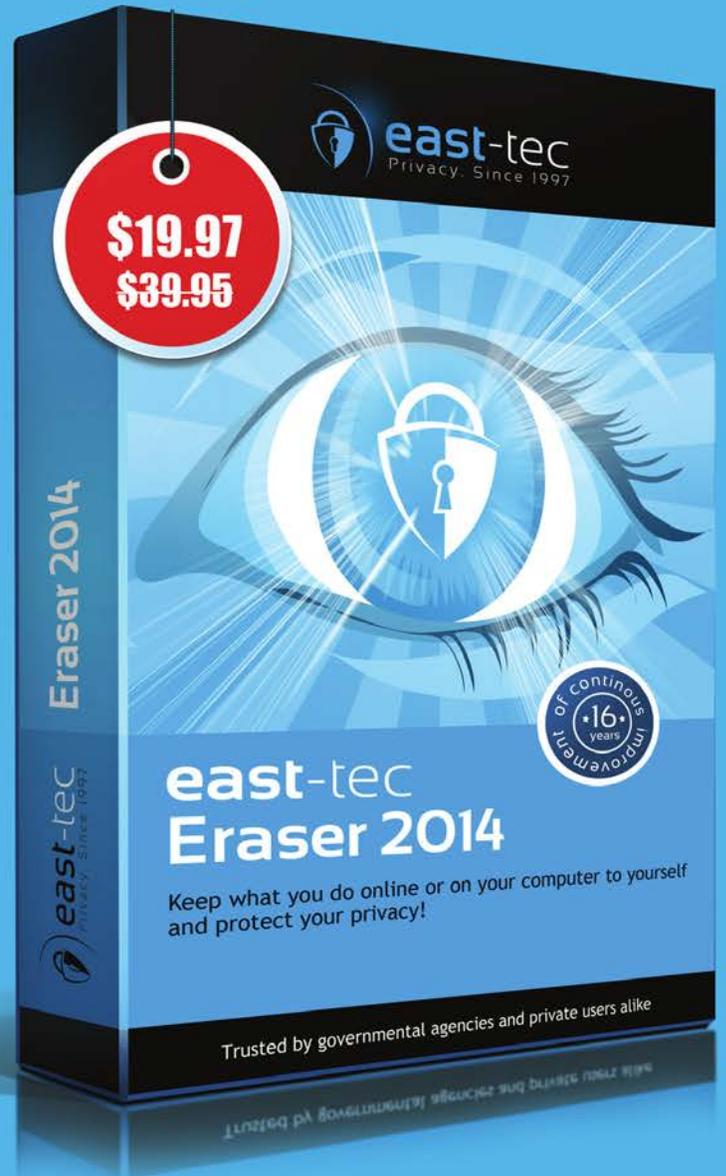
Cyber Defense Magazine - Cyber Warnings rev. date: 04/26/2017

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



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