CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IoT & DDoS

Cyber Security ROI

Ransomware Defense

Offensive Security

August 2016

MORE INSIDE!

CONTENTS

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Lukasz Szostak
Dave Larson
Avi Freedman
Jim Jaeger
Max Emelianov
Ram Vaidyanathan
Gary S. Miliefsky
Raj Samani
Milica Djekic
Philip Masterson
Tom Gilheany
Robert Capps
Cherif Sleiman
Tim Mullahy
Harpreet Bassi
Hussein Badakhchani
Matthew Davis
Theresa Payton
Kevin Poulsen

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Isn't It Time We Go On The Offense?

Friends,

With all the breaches happening today, shouldn't we get a bit more proactive? Let's analyze the root cause of breaches together, shall we? #1 we find that employees are easily tricked into opening attachments that come from cyber criminals. #2, we don't take the necessary precautions to reduce internal risks in our networking environments – this may be due to the fact that most in IT are understaffed and overworked. How could we let this happen to ourselves? With over $600B in cybercrime predicted for this year, with so many variants of successfully deployed ransomware, isn't it time we go on the offense and stop becoming victims?

As an INFOSEC professional, I highly recommend you ask your "C" level executives for bigger budgets for 2017 because it's only going to get worse. Get them to agree to allow you to begin more rigorous training of all personnel, especially those who keep becoming victims of spear phishing attacks. Also, I'm sure we all know the risk formula but are too busy to focus on the most serious risks to our organization – an upcoming breach – be it a malicious insider, a remote access Trojan siphoning personally identifiable information (PII) or other valuable information – we must become more vigilant. The breaches are reaching an exponential growth level. Remember that Risks to your organization start with Threats, Vulnerabilities and Assets. You must be better prepared for the latest threats. You must remove your most serious vulnerabilities that are easily exploited and you must ensure only healthy, trusted Assets are on your network.

In this edition of Cyber Warnings, you'll learn the 7 Secrets of Offensive Security. I would add a few to the author's list – one would be to learn about Honeypots at HONEYNET – visit them at https://www.honeynet.org/ The Honeynet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. With Chapters around the world, their volunteers have contributed to fight against malware (such as Confickr), discovering new attacks and creating security tools used by businesses and government agencies all over the world. The organization continues to be on the cutting edge of security research by working to analyze the latest attacks and educating the public about threats to information systems across the world. Another recommendation would be to keep on taking the latest INFOSEC and ETHICAL HACKER courses – stay on top of the latest trends and the best ideas. Finally, like we do here at CDM, share these ideas with your peers. Get together with fellow INFOSEC professionals whenever you can – if you are in Banking, start an INFOSEC Bankers meetup.

If you are in Healthcare, start an INFOSEC Healthcare meeting. Networking and communicating will lead to new ideas on how to get one step ahead of the next threat.

To our faithful readers, Enjoy

Pierluigi Paganini

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

Are we witnessing the rise of the Chief Marketing Security Officer?

By Lukasz Szostak

Just over four years ago Gartner famously predicted that by 2017 CMOs will spend more on information technology than CIOs. Recent industry reports suggest that what in 2012 sounded like a bold prediction, today becomes a reality and, according to a recent CIO.com article, CMOs already start outspending CIOs.

At the same time there has been a huge disconnect between marketing teams and technology teams. They operate with different mindsets, time horizons and goals; marketing teams are project driven, while traditionally IT has been process driven. A couple of missed campaign deadlines are usually enough a reason for marketers to externalize the next product microsite or a campaign landing page to their third party digital agency. It's a win-win – marketing get work delivered on time and IT don't have to deal with "those marketing people".

But where's information security in all this? Say your marketing launched a new product campaign run by a third party social media agency. Say that the agency created a campaign landing page on their servers to collect prospect customer data. What if the site gets compromised or your data spills over to your competitor's database hosted with the same agency?

This scenario could easily cost the CMO or the CISO a job, but marketing technology security still remains in the blind spot of most C-level executives.

It will only get worse

As more and more industries become commoditized, enterprises compete increasingly more by the means of Customer Experience. Forrester put it very bluntly in one of its press releases by saying that companies will "thrive and fail" in the age of the customer. The analyst firm also put "personalizing the customer experience*"* on top of the list of 10 critical success factors that will determine who wins and who fails in this new environment.

Kevin Cochrane, a veteran CMO in the marketing technology space addressed the same topic in his recent interview:

> *To win, you need to know the intimate details about your customers. From when they wake up to when they go to sleep and what dreams and aspirations they have. But, at the same time, that's the very same data that makes it so valuable to steal from you.*

To make matters worse, the regulators already stepped in, EU council leading the way with its General Data Protection Regulation that includes draconian fines for non-compliance - 4% of annual revenue or 20 million Euros, whichever is highest.

What it means is that it is no longer a choice whether marketing technology security is your priority – with fines as high as 4% of your annual revenue it is now a necessity.

So, zooming out for a moment, here's your 30,000 feet view:

1. Your business will succeed or fail depending on customer experience.
2. You can only win the customer experience game if you know everything about your customer.
3. Digital customer experience technology is in your CISO's blind spot.
4. A breach of customer data may cost you up to 4% of your revenue and, more importantly, can make you fail at the customer experience game.

What's next?

CMOs and CISOs are disconnected today in a similar way that CMOs and CIOs used to be. Even though this disconnect between IT and marketing still exists, it has been recognized years ago and it gave rise to the Chief Marketing Technologist. Marketing technologists stepped into the gap between the CMO and the CIO and have become one of the most sought after employees. According to VentureBeat, marketing technologist was the hottest job of 2015, right alongside data scientist.

Will the same happen in the marketing technology security space?

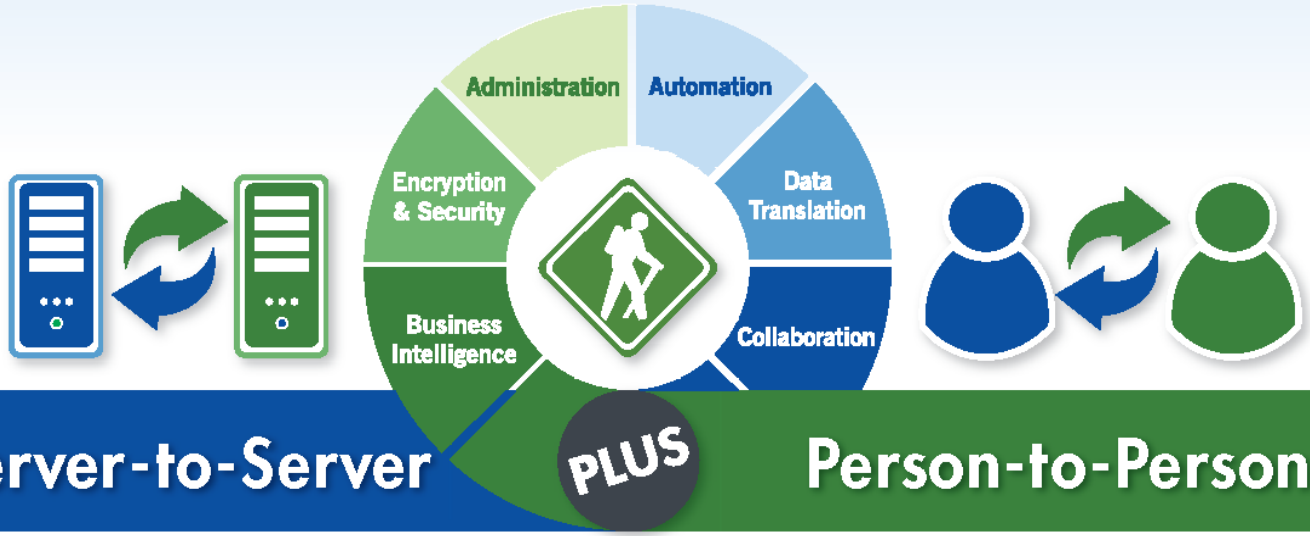
Are we facing the rise of the Chief Marketing Security Officer? That I don't know for sure, but what I know is that there is a void between the CMO and the CISO that someone will have to step into.

About the Author

Łukasz Szostak is an entrepreneur as well as a board member and partner at TBSCG, a global professional services and cloud computing group, which specializes in bringing the marketing and information technology worlds together.

Based in New York City, he has been in the marketing technology space since early 2000's, and enjoys writing about customer experience management, digital asset management and technology strategy.

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

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

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

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

Visit GoAnywhere.com for a FREE trial.

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

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

One of the Largest North American Railroads

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

GoAnywhere.com 800.949.4696

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

DDoS Attacks Present A Hurdle That the Internet of Things Has Yet To Clear

Securing the Internet of Things Against DDoS Threats

by Dave Larson, Chief Operating Officer, Corero Network Security

The internet has revolutionized the way we live, the way we do business and the way we stay "connected." Since the birth of the internet, technological advances have allowed us to mobilize our communications, automate everyday activities, enhance user experience and create an interconnected world in which we have come to rely on the Internet of Things (IoT).

We are experiencing a paradigm shift with the IoT – a global market that the research firm Gartner estimates is growing at a rate of 5.5 million new connected devices per day, and is expected to grow to 20.8 billion connected devices by 2020.

For businesses, IoT provides the opportunity for real transformation, allowing them to achieve new efficiencies and savings in their supply chain, gain access to more real-time data to facilitate faster and more-informed decision making tailored to a customers' needs or changes in the market and deliver new IoT-enabled products or services that grows their bottom line.

Internet-based home automation such as video baby monitors, remote thermostat programming, home surveillance and security kits, connected lighting products etc., are transforming how we manage our day-to-day lives. Remote management of these devices, through smartphones, online portals and the like has extended to every home, car, business, building and system in the world.

While one can argue that the term "IoT" is overused, misunderstood or perhaps represents a growth spurt in the evolution of technology, the increasing issue is the security of this phenomenon.

Research firm International Data Corp. expects the IoT market, currently pegged at $812 billion a year, to reach $1.46 trillion by 2020.

What we don't hear about as often, is how vulnerable these devices are when it comes to cyber-attacks. The average user of connected devices, whether that be your smart home, smart appliances, smart car or smart office, does not typically pay close attention to software updates or critical patching schedules.

They also don't quite understand how these devices are connected or sharing data. How the human component contributes to an overall lack of security of the IoT is often underestimated.

In the case of distributed denial-of-service (DDoS) attacks, the reality is that any device, infrastructure, application, etc. that is connected to the internet is at risk for attack, or even more

concerning, to be recruited as a bot in an army to be used in DDoS attacks against unsuspecting victims. Botnets, also known as “zombie armies,” can be deployed on thousands — if not millions — of connected devices and can wreak havoc - spam attacks, spread malware or launch DDoS attacks.

Commonly used DDoS toolkits abuse internet services and protocols that are available on open or vulnerable servers and devices, to create a class of attacks that are virtually impossible to trace back to the originating attacker, known as amplification DDoS attacks.

This raises serious concerns that the sheer number of devices in the IoT represents a totally new type of attack surface that could become wildly out of control in very short order.

There is really no limit to the potential size and scale of future botnet-driven DDoS attacks, particularly when they harness the full range of smart devices incorporated into our IoT.

By using amplification techniques on the millions of very high bandwidth capable devices currently accessible, such as baby video monitors and security cameras, DDoS attacks are set to become even more colossal in scale.

The bottom line is that attacks of this size can take virtually any company offline – a reality that anyone with an online presence must be prepared to defend against. And it isn’t just the giant attacks that organizations need to worry about.

Before botnets are mobilized, hackers need to make sure that their techniques are going to work. This is usually done through the use of small, sub-saturating attacks, which most IT teams wouldn’t even recognize as a DDoS attack.

Due to their size – the majority are less than five minutes in duration and under 1 Gbps – these shorter attacks typically evade detection by most legacy, out-of-band DDoS mitigation tools, which are generally configured with detection thresholds that ignore this level of activity.

This allows hackers to perfect their attack techniques, while remaining under the radar, leaving security teams blindsided by subsequent attacks. If these techniques are then deployed at full scale with a botnet, the results can be devastating.

Preventing and mitigating the exploitation of the IoT is going to take quite a concerted effort. Device manufacturers, firmware and software developers need to build strong security into the devices. Installers and administrators need to change default passwords and update patch systems – if this is even possible – when vulnerabilities do arise.

Organizations must also be better equipped to deal with the inevitable DDoS attack. An organization’s security posture is only as good as their ability to visualize the security events in the environment.

A robust modern DDoS solution will provide both instantaneous visibility into DDoS events as well as long-term trend analysis to identify adaptations in the DDoS landscape and deliver corresponding proactive detection and mitigation techniques.

Automatic DDoS mitigation is available today to eradicate the threat to your business and eliminate both the service availability and security impact.

About The Author

Dave Larson is the Chief Operating Officer of Corero Network Security. He is responsible for directing the Corero technology strategy as the company continues to invest in its next phase of growth; providing next generation DDoS attack and cyber threat defense solutions for the Service Provider and Hosting Provider segments.

Larson brings over 20 years of experience in the network security, data communication, and data center infrastructure industries. Most recently, Larson served as Chief Technology Officer for HP Networking and Vice President of the HP Networking Advanced Technology Group. In this role he was responsible for creating the long-term technology vision and strategy for HP Networking across a variety of product divisions and geographies.

Larson was instrumental in establishing HP's leadership in SDN including driving the creation of the OpenDaylight open-source SDN controller initiative as one of the founding executive sponsors of that consortium, along with technology leaders that included Cisco, IBM, NEC, Citrix and the Linux Foundation.

Under Larson's leadership, HP created the category for SDN security applications for enterprises as evidenced by the HP Network Protector SDN Application, which combines IP-reputation DNS security with HP's Virtual Application Networks SDN Controller to deliver botnet command-and-control and malware mitigation at the first touch point in the Ethernet access layer. Prior to that, he served as Chief Technologist for security and routing, and was a senior member of the Advanced Technology Group within HP Networking.

Prior to HP, Larson was Vice-President of Integrated Product Strategy for TippingPoint, where he was instrumental in transitioning the business to develop a line of Next-Generation Firewalls and vice-president of Security Product Line Management for 3Com Corporation where he defined global security products strategy across R&D development facilities in the U.S., U.K., and China.

Larson has also held senior marketing and product roles with Tizor Systems, Sandburst Corporation and Xedia Corporation. He has a Bachelor of Science degree in Physics from Gordon College in Wenham, Mass.

Dave can be reached online at LinkedIn and at our company website https://www.corero.com/.

Breakthroughs defining the future of wireless.

CTIA's Mobile Intelligence Conference

This cutting-edge conference is an open-dialogue program that's all about advancing "the art of the possible." Join the conversation and take away technical intelligence, best business practices and key insights into the issues and opportunities surrounding the super-connected life of tomorrow.

Tracks:

- Everything Intelligent: *Taking Networks to 5G*
- Everything Connected: *Smart City + Smart Consumer*
- Everything Enterprise: *5G Use Cases*
- Everything Policy: *How Washington Shapes Mobile*

Complete session descriptions at
www.CTIASuperMobility.com/education

ctia Super Mobility 2016™

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

REGISTER NOW CTIASuperMobility2016.com

Cyber Defense Magazine readers receive 20% off the EDUCATION PASS! Use promo code: CDM4INTEL

DDoS Defense: Can You Tell Friend from Foe?

By Avi Freedman, CEO of Kentik

In many organizations, networks are at the core of the business, enabling not only internal functions such as HR, supply chain, and finance but also the services and transactions on which the business depends for revenue. That makes network availability critical.

Any interruption of access from the outside world turns off the revenue spigot, impacting profit and creating a bad user experience that can damage customer satisfaction and result in permanent loss of patronage. The worse the outage, the worse the damage.

That's why speed is so important in detecting, diagnosing, and responding to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

One of the chief challenges in responding to an attack is to distinguish friend from foe. Without a way to drill down into traffic details and examine host-level traffic behavior, it can be difficult to tell the difference.

Traditional network analysis technologies based on pre-cloud architectures have been too limited in their compute and storage capacity to do more than perform pre-defined alerting and summary reports.

That's just not enough information to really get to the heart of what's happening in a complex networking scenario.

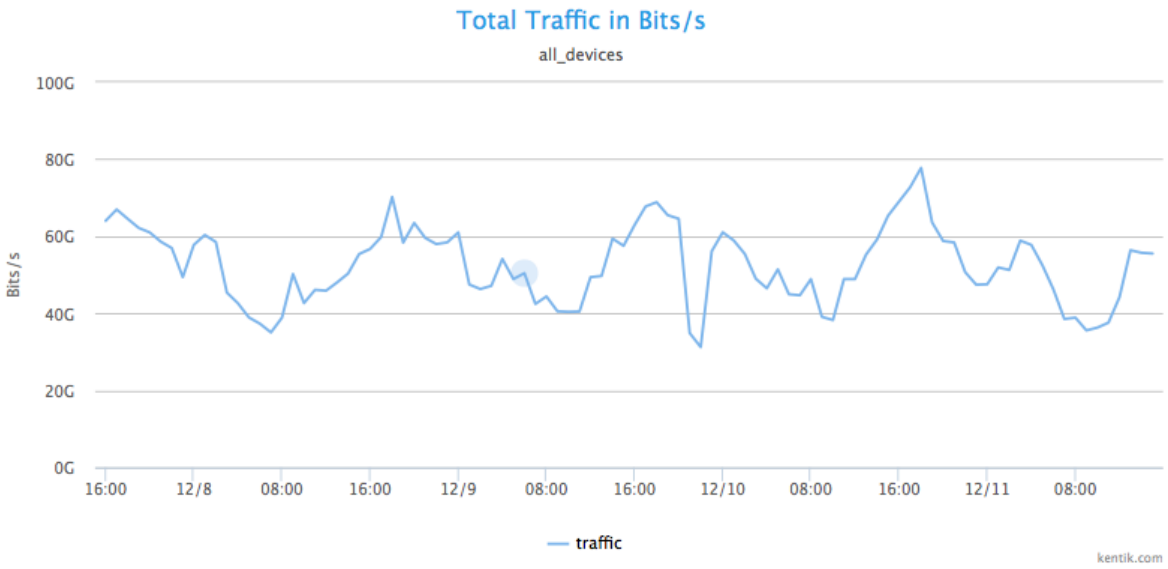
Fortunately, new big data techniques allow us to dig deep into huge volumes of network traffic details so that it's possible to understand what is really going on.

With a properly implemented big data platform, you can pivot your views of data to rapidly gain insight, in operational timeframes, so you can act to mitigate an attack or remediate a more innocent but still painful network issue.

We'll examine data that is readily available through common network traffic flow telemetry exports such as those provided by routers and switches enabled by NetFlow, sFlow or IPFIX.

Starting at the Top

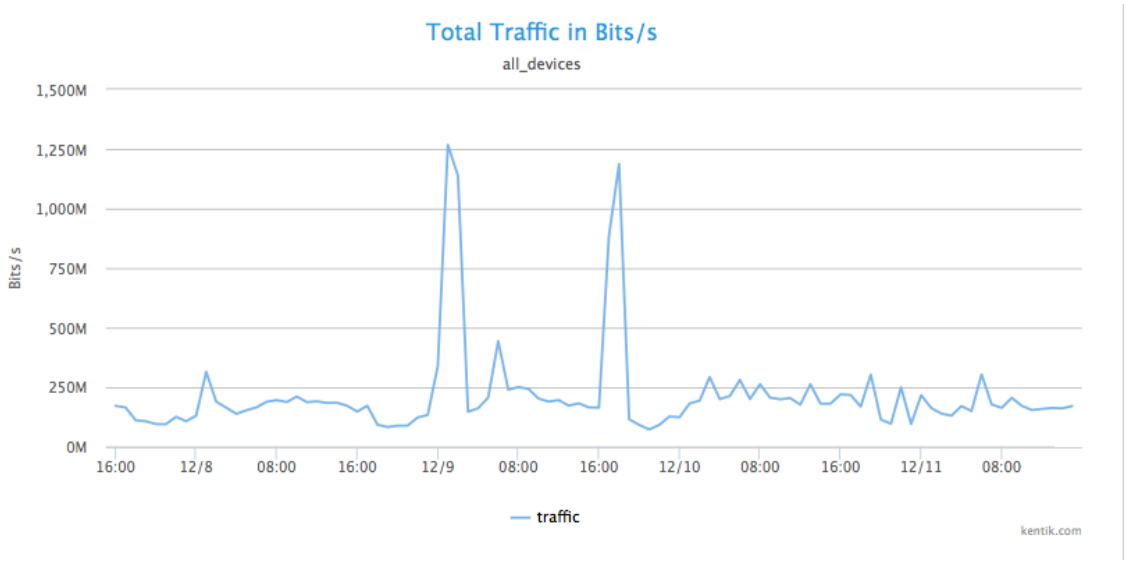
Let's say we're seeing symptoms of an attack in our infrastructure. We'll use traffic flow summary data to quickly scan total traffic in bits per second just to see if anything stands out.



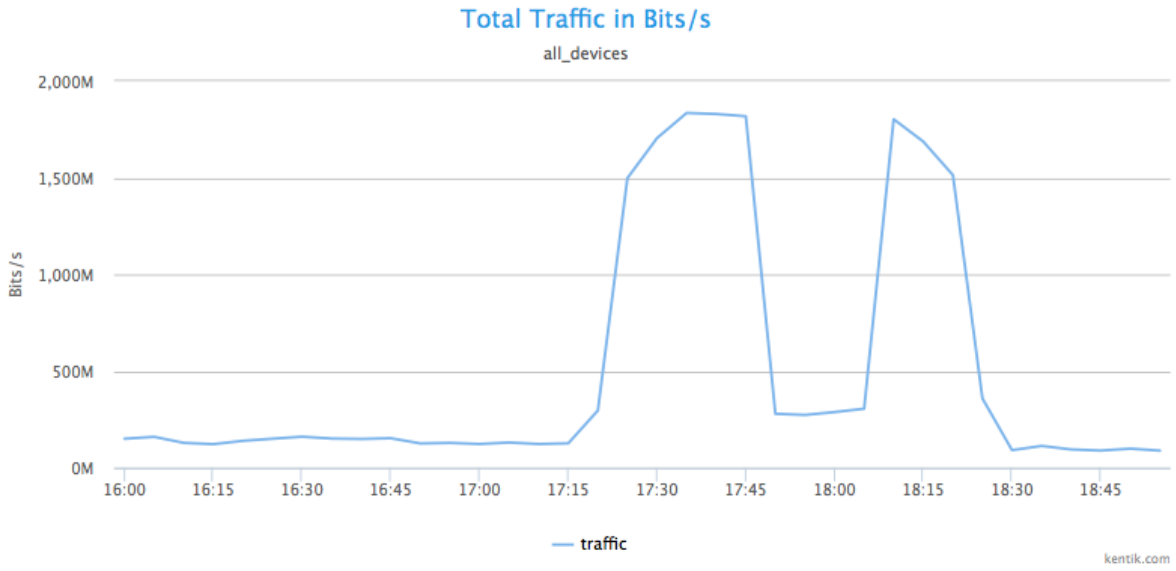
There's no obvious traffic spike from this view, but then again the network we're looking at is running at an average of 60 Gbps, so that doesn't mean there aren't worrying things going on at deeper levels of the network.

Analyzing Source Geography

One of the things that big data is good at is fusing many data sources together. By combining NetFlow data with GeoIP, we can look at traffic by source geography. In this case, the network doesn't get a lot of traffic from China, so what happens when we filter total traffic by China as source.

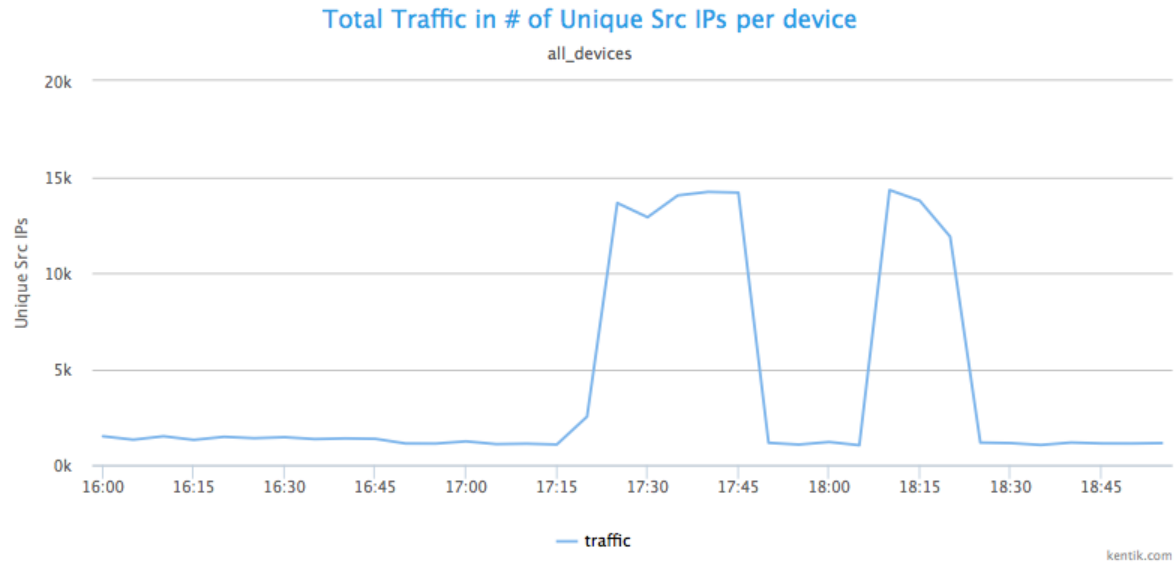


Aha! That analytical pivot produces a graph above, showing two obvious spikes that are well above average. Below, we zoom in on the time of the spikes.



Analyzing Unique Source IPs

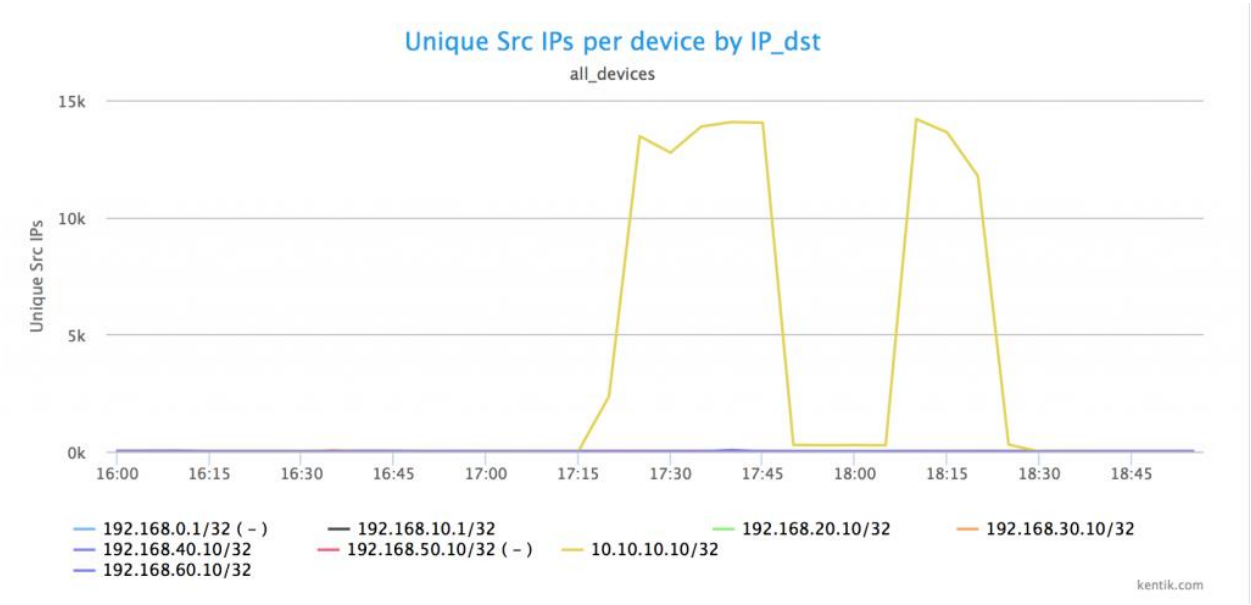
The spikes themselves are suspicious, but is this just a large data file transfer? We can find out by looking at how many different source IPs are sending traffic. To look at host-level details, note that we've gone beyond the point where you can use summary information. At this point, we are analyzing raw NetFlow record details.



Those raw NetFlow details sure are useful, because there is in fact a huge increase in the number of unique source IP addresses sending traffic to particular destination IPs. This tells us that we're not looking at a large file transfer from a single machine, but a highly distributed set of senders. Botnet much?

Who's Getting Hammered?

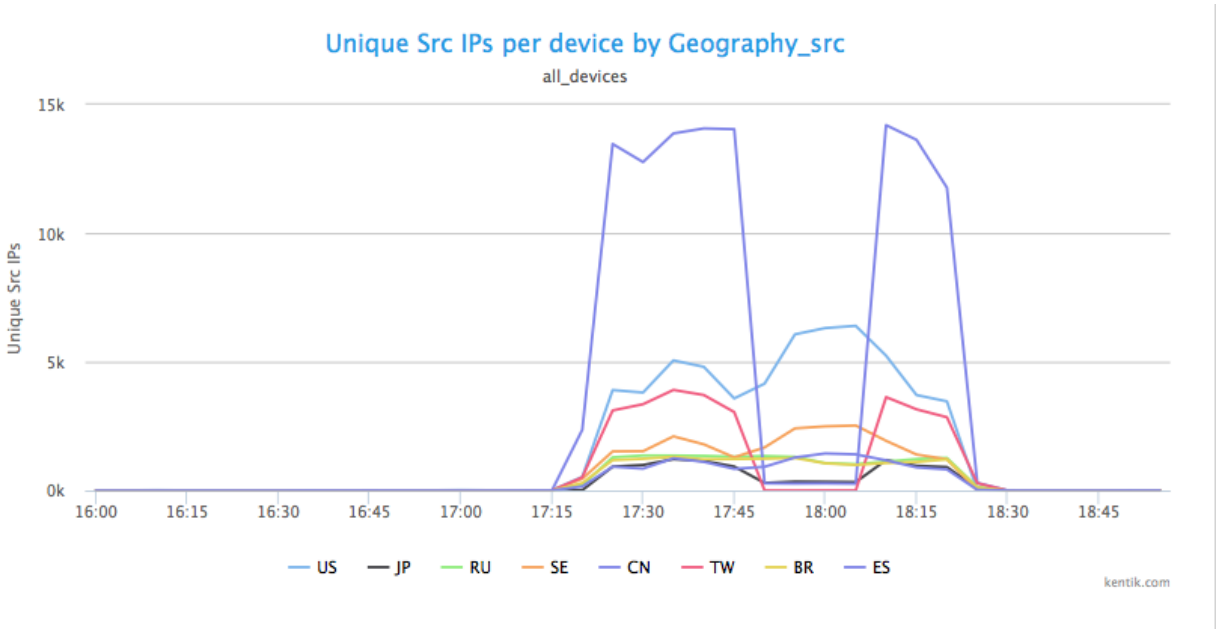
The next step is to determine which IP or IPs are getting all this (probably unwanted) traffic from 14,000 or so individual host IPs.



The ability to dig into high volumes of host-level NetFlow details again proves its utility. We can see that the main target is a solitary destination IP address: 10.10.10.1 (actual address anonymized to protect the victim). There's really only one likely explanation for traffic from thousands of hosts in a country which you have no business dealings with, to a single IP, that suddenly spikes from nearly nothing to more than 1 Gbps: This is a DDoS attack. Note that this isn't a mega attack, but it can still cause real problems for whatever is running on that individual host, and anything else that depends on it. If it's your DNS server, it might make it impossible for lots of other servers and applications to function.

Going Deeper

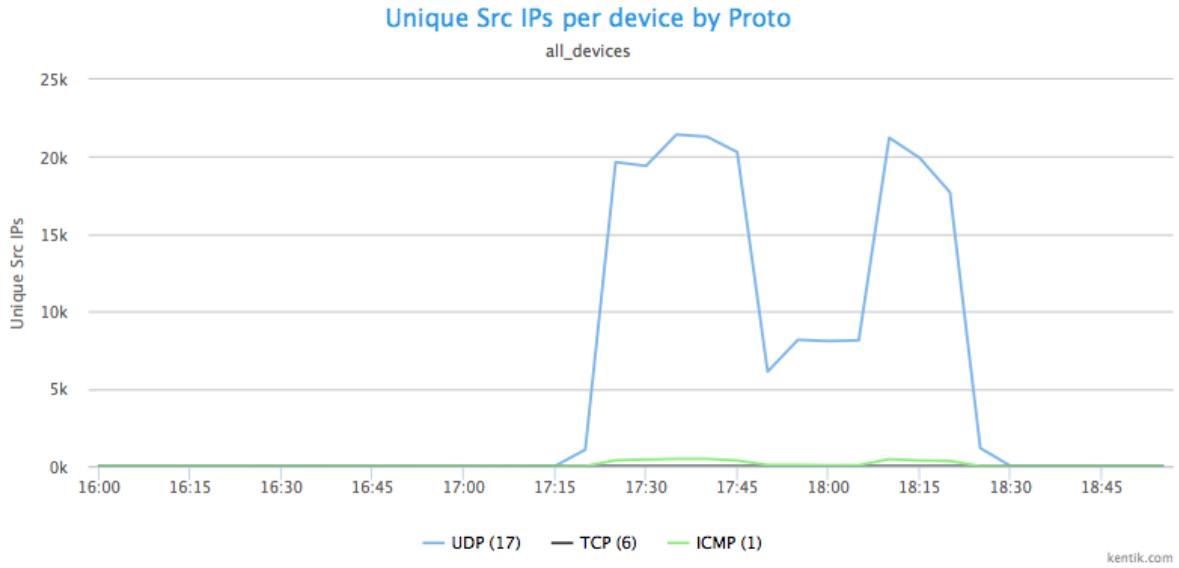
Now that we know it's a DDoS attack, we shouldn't stop because what if that attack is coming from other countries besides China? We pivot our analysis again to widen our lens.



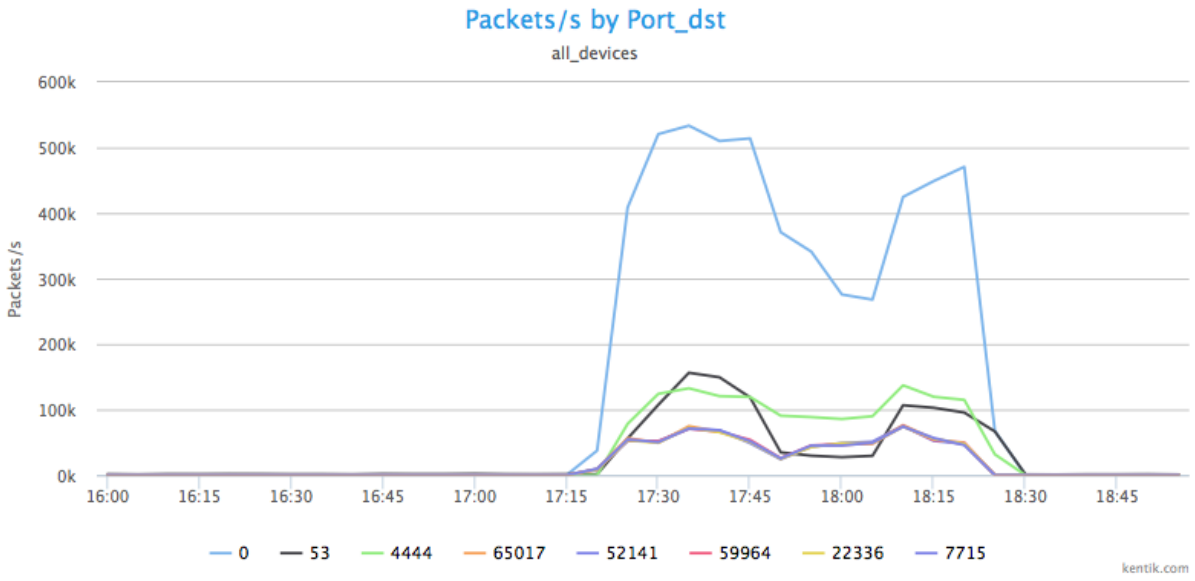
Lo and behold, there is indeed DDoS traffic coming from multiple countries, including the U.S., Japan, Russia, Sweden, China, Taiwan, Brazil, and Estonia. Good to know.

Characterizing The Attack

Next we want to know specifically what type of traffic we're seeing and what that tells us. We'll group the traffic coming from all those source host IPs by protocol.



Clearly, this is UDP-based attack. Now we'll look at the destination port(s).



We can see that the UDP traffic is being sent to multiple ports, and it's obvious that we're experiencing a DNS redirection/amplification attack occurring on port 53, with a lot of port 0 UDP packet fragments being generated as collateral traffic.

Is There Something Underneath This Volumetric Attack?

So far we've gotten a lot of insight into the details of the DDoS attack from full NetFlow details. But is this volumetric DDoS the main event, or are we being distracted from looking for other, less obvious threats? We can see a lot of packets being sent to port 4444 (green line in graph).

Port 4444 is the UDP port for the Kerberos service, and is — at least for Windows machines — a well-known target for buffer overflow attacks, often used to insert trojans such as Hlinic and Crackdown.

So, there are potentially two types of attacks going on in parallel: a DDoS attack and a buffer overflow trojan insertion. Many security blogs and publications note that DDoS attacks are often used to obfuscate other exploits. This may very well be an example of that technique.

Getting a Handle on Attack Mitigation

Characterizing the attacks leads us to mitigation. One way is to take the attack traffic and group it by /24 source network addresses:

ipv4_src_addr	Avg pps	Percent Total	95th Percentile	Max pps
1.214.125.0/24 (-)	1,144	0.21	5,981	5,981
103.15.244.0/24 (-)	1,058	0.20	9,012	9,012
95.163.106.0/24 (-)	832	0.16	3,796	3,796
103.246.64.0/24 (-)	690	0.13	4,615	4,615
61.89.225.0/24 (catv61-89-225-0.sensyu.ne.jp)	581	0.11	3,441	3,441
212.77.210.0/24 (-)	539	0.10	3,496	3,496
61.111.6.0/24 (-)	534	0.10	3,414	3,414
126.42.120.0/24 (softbank126042120000.bbtec.net)	491	0.09	2,322	2,322
96.89.110.0/24 (-)	481	0.09	1,775	1,775
125.191.127.0/24 (-)	478	0.09	2,813	2,813
103.251.48.0/24 (-)	469	0.09	2,403	2,403
4.28.72.0/24 (-)	467	0.09	2,240	2,240
211.234.111.0/24 (-)	459	0.09	1,967	1,967
115.95.114.0/24 (-)	437	0.08	2,403	2,403
182.226.45.0/24 (-)	433	0.08	2,868	2,868
203.109.129.0/24 (-)	433	0.08	1,694	1,694
118.163.181.0/24 (118-163-181-0.HINET-IP.hinet.net)	425	0.08	2,840	2,840
182.226.201.0/24 (-)	407	0.08	2,649	2,649
186.208.192.0/24 (-)	400	0.08	2,158	2,158
50.250.114.0/24 (50-250-114-0-static.hfc.comcastbusiness.net)	391	0.07	2,485	2,485

We can now take two mitigation steps:

Ask our upstream ISP to drop this traffic or send it to a scrubbing service or device if we have one

As an added precaution, drop all traffic from these countries going to port 4444 on our own routers

Conclusion

One of the benefits of being able to dig into full-resolution NetFlow data is that you can get operationally useful insights without needing in-line devices. You also get more freedom to employ a portfolio of mitigation methods.

At Kentik, we're big believers in the power of network data. Rather than summarize and FIFO raw NetFlow data, we augment raw inbound NetFlow records with BGP, GeoIP, and other datasets, then store that expanded dataset at full resolution for 90 days in our cloud. It's possible to do this type of thing with open source tools, or use a service like ours if you don't want to DIY. Either way, big data is the way forward if you want to have full details at your disposal in order to deal with DDoS attacks.

About the Author

Kentik Co-Founder and CEO Avi Freedman has decades of experience as a leading technologist and networking executive. Prior to co-founding Kentik in 2014, he served in several roles for Akamai, including Chief Network Scientist and Vice President of Network Infrastructure. In 1992, Freedman launched Netaxs, the first ISP for Philadelphia, before going on to serve as the Network Director for AboveNet and the CTO for ServerCentral.

R3: Resilience, Response & Recovery Summit 2016

Etc Venues St Paul's, London

27 September 2016

50% off for *Cyber Defense Magazine* readers

Your roadmap to a robust incident response plan

The R3 Summit takes you through the most vital steps of your response and recovery strategy, sharing practical takeaways alongside legal guidance and incident exercises.

In its second year, the R3 Summit brings you:

150+ information security professionals • 20+ top-notch speakers • 6 how-to guidance sessions • 2 case study sessions • 2 spotlight sessions • 1 cyber-breach simulation • 1 set of collaborative roundtable discussions • 1 hands-on workshop • 1 head-to-head session • 1 friendly fireside chat • 1 champagne reception with 150+ networking opportunities

This is your chance to **join industry professionals** across business sectors to meet and exchange **best practices** on recovering from data breaches and **creating first-rate responses** to them.

For more information and to register, please visit our website, call Tracey on **020 8349 6475** or email **tracey.m@business-reporter.co.uk** claiming your 50% off with promo code **MP50**

www.r3summit.co.uk

BR

Building a Business Case for Security that the CFO Can Understand

Jim Jaeger, Chief Cyber Services Strategist, Fidelis Cybersecurity

According to a March 2016 PwC report, 'A False Sense of Security?', that surveyed 300 Middle Eastern organizations, the region has become one of the prime targets for cyber-attacks.

In fact, according to the findings in the report, in 2015, 56% of businesses in the region lost more than US$500,000 as a result of cyber incidents compared to 33% globally.

Faced with this reality, organizations across the region have upped their IT security spend. However, one of the biggest challenges when you go shopping for new security tools is answering the inevitable question from finance: "What's the value?"

Determining the ROI of a new security product isn't an exact science. There are no hard and fast rules to follow – which is why generic ROI calculators should be avoided at all costs (pun intended).

Measuring the impact of better security is like measuring a moving target. What's more, every organization is unique.

The setup of an organization's existing infrastructure, its size, risk level and the potential impact of a security incident, will vary significantly. Ultimately, this means that successful security strategies can look very different.

Where is the value?

On the face of it, most security tools don't appear to save you time or money. They generate new alerts and this can swamp an already overburdened security team with investigating and tracking down new potential threats.

That's not to say that security tools have no value, however, and it's by evaluating this that a CFO can understand the true business case for a security solution.

However, the challenges inherent in defining the ROI for security tools does not decrease the importance of defining this information and articulating it for corporate leaders and the Board.

The recent explosion in the number of security vendors in the market, offering similar overlapping solutions, and their almost identical claims to "solve the security problem" makes picking a comprehensive security solution more difficult.

The fact that its increasingly difficult for CIOs and CISOs to understand if and where security gaps still exist, doesn't decrease the importance of helping C-suite executives and Board

understand the value of proposed security programs and the importance of resourcing them.

In security, the biggest benefit will always be reduced risk; “buy this tool (or hire this person) and bad things are less likely to happen.”

Unfortunately, this argument is highly theoretical, which doesn’t translate easily into a business case.

It’s also likely that the same argument has been used for previous security procurements and consequently leads to a debate around the likelihood of data being stolen – a risky game to play.

Instead of trying to estimate the level of risk a company has in terms of security and how likely an attack may be, it’s arguably much more important to analyze the time and/or people a new tool might save and how much more efficient it could make an organization.

Some key questions would be:

- Can it automate tedious day-to-day activities?
- Can it reduce requirements for highly skilled, difficult to hire security personnel?
    - Will it let tier 1 analysts do the tasks of a tier 2 analyst?
    - Will it allow tier 3 analysts to do the work of an incident responder?
- Does it reduce the time it takes to resolve a threat?
- Will it help consolidate the security stack e.g., reduce the number of agents operating on endpoints or the number of network security appliances in your rack?
    - Will it reduce the requirements to integrate multiple security devices?
    - Will it reduce the number of screens that monitoring personnel have to focus on?
- Can it improve the speed and accuracy of a company’s incident response?

To the CFO, this approach presents clear opportunities to save critical funds and enhance the ROI of security solutions.

At the same time, you are reducing the risk to the enterprise of a breach which is a primary focus of the Board of Directors.

For any organization it is almost impossible to put a prediction on how much a cyber breach could cost as it isn’t only a case of compensating victims and the loss of business revenue, but also damaged reputation.

No one is expecting a CFO or the Board to write a blank check for security, which is why explaining the savings an enterprise can make in terms of a more efficient security team, lower hardware costs, and minimized risk, is paramount to understanding its value.

About the author:

As an esteemed security leader, Jim Jaeger is responsible for developing and evolving the company's cyber services strategy and business.

He brings expansive cybersecurity expertise, encompassing an impressive, high ranking career in the U.S. Air Force and driving advanced cyber programs at federal agencies while at General Dynamics.

Most recently, Jim managed and grew Fidelis' Network Defense and Forensics business, including the Digital Forensics Lab. He has led cyber forensics investigations into some of the world's largest network breaches impacting our industry. In 2015, Rhode Island Governor Gina Raimondo appointed Jim to the state Cyber Commission.

Mr. Jaeger has also held leadership roles for a wide range of cyber programs including General Dynamics' support for the DoD Cyber Crime Center (DC3), the Defense Computer Forensic Lab and the DefenseCyber Crime Institute.

Previously, he created General Dynamics' information assurance and critical infrastructure protection group, which has developed a wide variety of Information Assurance tools, ranging from the Air Force's intrusion detection infrastructure to the only network based multi-level security (MLS) system, accredited by the National Security Agency at Protection Level 4 without waivers.

He is a former Brigadier General in the United States Air Force and his military service includes stints as the Director of Intelligence (J2) for the U.S. Atlantic Command, Assistant Deputy Director of Operations at the National Security Agency, and Commander of the Air Force Technical Applications Center.

In these capacities, Jim was responsible for the collection and reporting of intelligence to Theater Commanders and the National Command Authority.

He received his Bachelor of Science degree from the Air Force Academy and his Master's degree in Management & Supervision from Central Michigan University.

He also completed the Executive Development Program at the Whitmore Graduate School of Business, University of New Hampshire.

THE COMMERCIAL UAV SHOW ASIA 2016

1 – 2 September 2016,
Suntec Convention Centre,
Singapore

DEMONSTRATING REAL WORLD APPLICATIONS OF UAV'S

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

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

FEATURED SPEAKERS

Claus Nehmzow,
Digital Innovation Organization,
BP, Singapore

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

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

TOP SPONSORS & EXHIBITORS

SPONSORS:

ALTA DEVICES
delair-tech
senseFly a Parrot company
YUNEEC AVIATION TECHNOLOGY

EXHIBITORS:

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

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

Five Things You Can Do To Protect Your Systems From Ransomware

Ransomware may soon become one of the most popular cyber attack methods. Don't let yourself get caught unprepared. Here's how you can ready yourself against it.

by Max Emelianov, CEO, HostForWeb

Earlier this year, the FBI reported that ransomware incidents are on the rise. No matter what industry you work in, you should be concerned. After all, virtually every business has data that's mission-critical; every organization has information which, should its employees lose access, could cause regular operations to come grinding to a halt.

For the uninitiated, ransomware is a particularly nasty type of malware which locks down access to any systems it infects. When a victim attempts to use an infected device, they'll generally be presented with a message - usually an account that they or their organization can forward money to in order to regain access to their stuff. These ransoms are almost always in bitcoins, and can range from a few hundred dollars to tens of thousands - one hospital had to pay $17,000 to regain access to its patient data (which probably pales in comparison to how much money they lost while their systems were locked down).

Suffice it to say, you need to take the necessary steps to protect yourself. That's where we come in. Today, we're going to go over some of the things you can do to guard against ransomware, no matter how it infects you.

One thing before we get started. We've not included patching and regular backups on this list, because we believe **that's something that every enterprise NEEDS to be doing anyway.** If you aren't keeping an eye on security updates, none of the advice we've laid out here will really be of use to you.

Keep Backups (And Keep Them Separate From Your Network)

A ransomware attack relies upon holding critical files hostage - therefore, the best way to protect yourself against them is to keep regular, automated external backups. That way, if access to files are locked down on your local network, you can simply format the infected systems and restore them to working order from your backups. Of course, the criminals who code ransomware know of this weakness - their viruses are often coded to seek out backup systems.

That's why it's imperative that you keep your backups separate from your local systems, either on the cloud or on an isolated, offline device. It's no good having backups if you get locked out of **them** at the same time as your other systems, after all.

Authenticate All Incoming Email

It should come as no great surprise to you that email is one of the chief delivery vessels for malware. All it takes is one employee foolishly downloading an attachment they shouldn't, and bam - your network's infected, and you're desperately running damage control. To guard against such a mode of attack, you need to protect your email servers.
There are a few steps in doing this, according to Information Week:

1. Make use of technologies like Sender Policy Framework, Domain Message Authentication Reporting and Conformance, and DomainKeys Identified Mail. This will allow you to mitigate attempts to spoof domain names or IP addresses, and make it harder for attackers to pose as legitimate senders.
2. Scan all stored, incoming, and outgoing mail with a trusted security suite or antivirus program. Attackers can use legitimate servers to launch an attack just as easily as spoofed servers, after all.
3. Train your employees to recognize the common elements of a phishing scam, and devise a response plan that you can put in motion in the event of an infection.

Monitor Everything

Beyond monitoring your email account, keep a close watch on all file activity that takes place on your servers. If you notice anything suspicious - rapid changes to your files, unusual sharing activity, or bizarre network traffic - you can lock things down. This will allow you to mitigate the damage the ransomware might cause; instead of allowing it to infect your entire network, you can isolate the infection to a system or two.

Ad Blockers Are Your Friend

Like it or not, advertisements are right up there with email as one of the most common delivery mechanisms for malware. And as demonstrated by the recent controversy with Forbes' ad-light experience, publishers cannot be trusted to effectively police their advertising networks. By installing ad blockers on all of your systems (and advising your users to do the same with any personal devices), you'll put a lid on one more potential attack vector.

Tweak Your Settings

Last but certainly not least, there are a few settings you can tweak and modify to effectively neuter most of the leading ransomware tools.

- *Open .JS files with Notepad by default.* There's a surprising volume of malware that uses JavaScript as a delivery medium - by setting JS files to be opened with Notepad (and not run automatically), you can effectively neuter such malware.

- *Display file extensions at all times:* Plenty of malware works by obfuscating the file extension or filetype. By setting your system so it displays extensions, you can ferret those malicious apps out.

- *Disable macros in Office documents.* Self-explanatory. Most of the time, you won't need macros.

- *Disable administrative permissions for regular users.* Although ransomware **can** run without elevated permissions, preventing regular employees from running apps as administrators can prevent it from encrypting everything - it'll only lock down files that the infected user can access.

- *Disable RDP*. The Remote Desktop Protocol is a frequent attack vector for many of the most popular ransomware tools - disable it if your employees don't require it as part of their workflow.

- *Limit access.* Do end users really need to access every mapped network drive in your organization? Probably not.

Closing Thoughts

Like it or not, cybercriminals are getting craftier. They've realized that while they can **certainly** steal and sell sensitive files like healthcare records or financial documents, it's often far easier to simply hold those files for ransom. After all, you'd be surprised what some people will pay when their business is on the line.

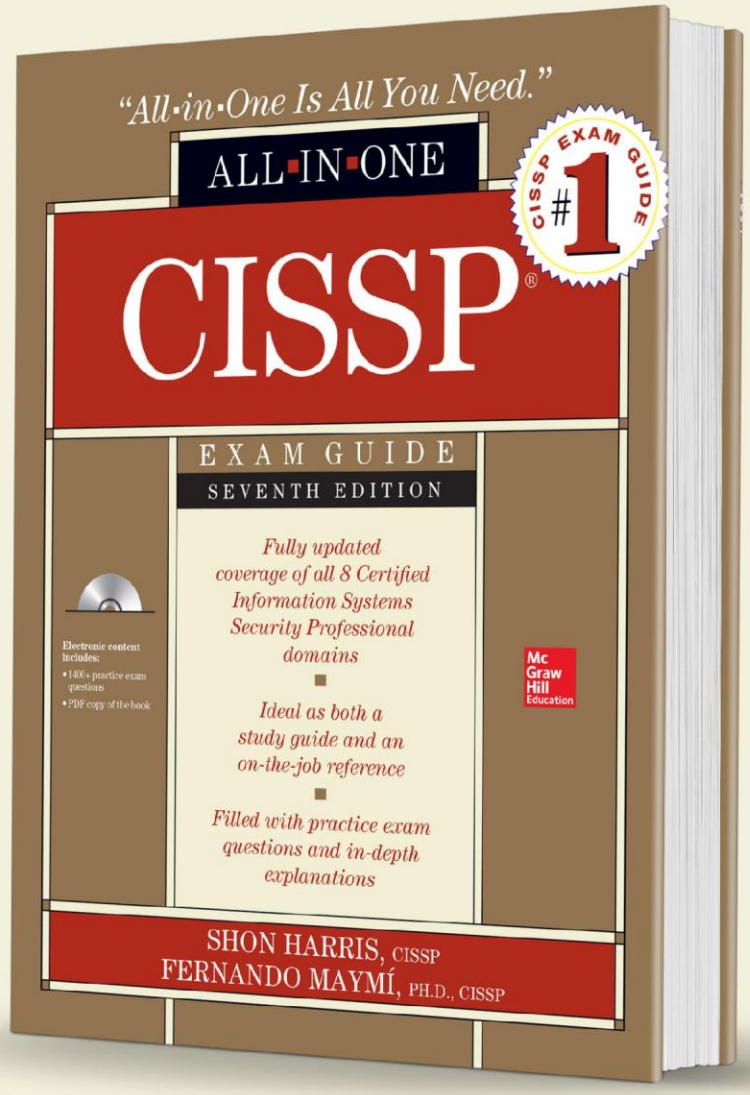
By following the steps we've outlined in this piece, you can effectively protect yourself from all but the worst ransomware. Just remember one thing, though: **no organization is completely immune to attack.** Complacency is your worst enemy here; above all else, you need to stay vigilant.

About The Author

Max Emelianov started HostForWeb in 2001. In his role as HostForWeb's CEO, he focuses on teamwork and providing the best support for his customers while delivering cutting-edge web hosting services. Max can be reached on Twitter at *@HostFW.*

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

SAVE 30%!



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

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

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

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

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

SAVE 30% at www.mhprofessional.com
with promo code CISSP0716

@MHComputing

Available in print and as an eBook

Mc Graw Hill Education

How To Combat Security Cracks Created By Collaboration

By Ram Vaidyanathan, ManageEngine

The number of cyberattacks will grow as employees increasingly use collaboration tools to maximize their company's productivity

Cybercrime costs the global economy as much as $450 billion each year. And, the median cost of cybercrime has increased by nearly 200% in the last five years.

Meanwhile, collaboration has become the cornerstone of successful organizations. But collaboration often comes with a risk.

The number of cyberattacks will grow as employees increasingly use collaboration tools to maximize their company's productivity.

This is because these tools can provide new points of entry for hackers looking to cause damage. This issue could become more serious as we will see more radical collaboration tools in the days to come.

Fortunately, there are always going to be readily available solutions. Here are three ways in which an organization's security can be compromised due to increased collaboration:

A wolf in sheep's clothing: Companies collaborate with suppliers, vendors and customers in the cloud every day. Consider this scenario: A supply chain executive receives an automated weekly email with an MS Excel file from their logistics partner, giving the estimated time of arrival for products. A cybercriminal somehow discovers this practice. The criminal then impersonates the logistics partner by using a similar email address.

The executive doesn't notice and downloads the attachment — an executable (.exe) file masked as an MS Excel file. When the executive opens the file, a wolf in sheep's clothing enters the company's network to steal trade secrets, financial data, and customer information. This modus operandi, called spear phishing, is popular globally. By some estimates, 91% of all attacks begin with spear phishing.

A betrayal: With the advent of bring your own device (BYOD), collaboration has become fairly common. Employees can now access work files while away from the office and increase their productivity. On the other hand, disgruntled employees can easily expose information or even sabotage company files.

What if an employee who is about to join a competitor were to print customer contact details from a remote location? And what if this employee took this information to the new workplace? This betrayal could lead to the company losing its competitive edge.

A foreign adversary: Even governments are not immune to cyberattacks from foreign state-sponsored adversaries. Government employees may visit certain websites frequently to collaborate with employees from other departments or with their citizens.

Malware placed on these sites could exploit vulnerable endpoints and compromise the devices of any visitors. Malware can also morph into more serious advanced persistent threats (APTs) that can lurk in the victim's system for a long time.

This way, these adversaries could secretly keep a tab on issues of national security and international policy. When governments can face such threats, businesses are all the more at risk.

To fight data breaches and defend their business, organizations must protect all entry points. Here are few ways in which organizations can defend against each of the threats identified above.

- Guarding the door: Application white listing, a method of checking applications against an approved list, is effective against criminals in disguise looking for an entry point. If an unknown program tries to run, it will be barred.

  This is very effective against spear phishing attacks. In addition, a log management system would help to collect logs on failed access attempts and decipher whether or not they are attacks.

- Guarding from inside: A privileged password management process can help organizations protect against insider threats.

  All privileged identities and passwords are stored in a centralized vault and only approved devices are allowed to access information from remote locations.

  Furthermore, companies can video record all sessions, whether on-premise or remote, for a complete record of all actions.

- Defending against international threats: Software applications that analyze packet flow can detect malicious traffic hitting the network in real time.

  In case of a sophisticated attack, the company can immediately view the offender's IP, the severity of the attack and the time of the attack.

  A detailed forensic investigation will enable the company to detect patterns and identify the source of unwanted intrusions.

In the present age of heightened collaboration, the risk of cybercrime is very high. Organizations need to defend against techniques such as spear phishing, malware and APTs, among others.

Application white listing, privileged password management and network behavior anomaly detection are just three modes of defense.

And what happens in a future of radical collaboration tools?

Future collaboration tools will be even more powerful. For example, the combination of holography and brain decoding technology may create a society in which people have meetings between their virtual selves in the office.

What if a cybercriminal impersonates a CEO's virtual self and compromises the business by giving wrong instructions during a meeting? In a scenario like this, even if a criminal were somehow able to project the CEO's hologram inside the office, the ICT team could detect the deviation if there were inconsistencies with the CEO's known logic.

There is no doubt that the future holds endless possibilities for collaboration, which we know to be integral for business success. We just need to make sure our security technology is well equipped to handle it.

However sophisticated the attacks in an age of increased collaboration, a proactive ICT team will always prevail.

About the Author

Ram Vaidyanathan is an IT evangelist at ManageEngine, the real-time IT management company. Ram closely follows emerging industry trends and is a frequent blogger on technology topics.

His main interest is in the impact of the Internet of Things on IT management. He has an MBA from the Schulich School of Business.

For more information on ManageEngine, the real-time IT management company, please visit www.manageengine.com; follow the company blog at http://blogs.manageengine.com, on Facebook at http://www.facebook.com/ManageEngine and on Twitter @ManageEngine.

CI CONNECT

Cyber Security Connect North America

Nov. 15, 2016 | Marriott at Metro Center | Washington, DC

An Invitation-Only Forum for Senior Executives in Cyber Security across North America. Hear from industry experts, including:

Nickolas Savage
Supervisory Special Agent (SSA)
Federal Bureau of Investigation (FBI)

Vivek Khindria
Director, Information Security
Bell Group of Companies

Jon Boyens
Senior Advisor for Information Security and Program Manager, ICT Supply Chain Risk Management, **National Institute of Standards and Technology (NIST)**

Drew Morin
Director, Federal Cyber Security Technology and Engineering Programs
T-Mobile US, Inc.

Rob Fry
Senior Security Architect
Netflix

Richard Starnes
CISO
Kentucky Health Cooperative

TO APPLY, PLEASE VISIT: **CanadianInstitute.com/Cyber**

7 Secrets of Offensive Security

Information Security (INFOSEC) Best Practices for Data Protection and Compliance

by Gary S. Miliefsky, CEO, SnoopWall, Inc.

The State of Network Security Today – Reactive and Slow

Network breaches are in the news every day. In the US alone, there have been over 900,000,000 – that's 900M records of personally identifiable information (PII) stolen over the past few years. While most organizations are running the latest corporate firewalls – also known as UTMs – unified threat management systems or NGs – next generation firewalls and the latest and greatest antivirus products, they are still breached.

Over 95% of breaches happen behind these corporate firewalls on these endpoints that appear allegedly to be secured by antivirus. So, it seems, the hackers have leap-frogged most INFOSEC countermeasures. Yes, that's what the tools you've been buying to protect yourself are – just reactive technologies, countermeasures, that usually react too late – causing a ransomware payment decision, data theft, downtime or even much worse.

The Way to Win the Battle – Proactive, Offensive, Fast and Semi-Automated

While not all of your defenses can be automated, I do like to focus on more proactive approaches to the problem of being breached. If you do a root-cause analysis, you will discover your weaknesses in advance of their exploitation. For example, let's say you buy the latest and greatest antivirus software, keep it always up to date and then get infected.

The infection exploits a fairly new but known vulnerability in the Microsoft Windows RPC protocol, which can be found in the nvd.nist.gov database on common vulnerabilities and exposures (CVEs). While your antivirus software focuses on reacting – scrubbing and cleaning up after you've been infected, it's still reactive technology.

The Offensive security model suggests you should find out which systems have the RPC vulnerability, contact Microsoft for a patch and fix this hole quickly. If there is no patch available, maybe you could turn off the RPC protocol for a few days or a week until next week's Patch Tuesday from Microsoft. This may cause a minor disruption in network service access or Remote Help Desk software, however, your Windows computers won't be getting infected with this new virus.

So, simply put, finding the leak and patching it or hardening the system is a lot better than bailing out water from a sinking ship because you never noticed it had this hole allowing the ship to fill with water.

Let's explore the 7 secrets of Offensive Security and learn a new, more proactive approach to dealing with protection of PII, keeping networks running and employees productive. We'll dig into ideas and methods that, while they sound so simple and easy, sometimes to implement them, you'll be dealing with corporate politics, budget issues, resource issues and time constraints.

I'll go into a deep dive for you on each of these seven secrets, however, let's get started right away, here are my seven secrets:

1. DEMAND EXECUTIVE SUPPORT – FUNDING, TRAINING, ETC.
2. DEPLOY CONTINUOUS (or daily at minimum) BACKUPS and TEST THEM – DOES THE RESTORE EVEN WORK?
3. DEPLOY CORPORATE WIDE ENCRYPTION
4. CREATE A "LIVING" CORPORATE SECURITY DOCUMENT
5. TRAIN (and RETRAIN) ALL EMPLOYEES ON BEST PRACTICES INFOSEC POLICIES (ISO27001, COBIT, NIST – choose one you like)
6. MANAGE THE BRING YOUR OWN DEVICES (BYOD) DILEMMA BY ASSUMING ALL MOBILE DEVICES ALREADY INFECTED
7. DEPLOY AND MANAGE A BREACH PREVENTION SOLUTION (we'll quickly show you ours) that helps…
    a) Document and mitigate RISK, especially serious vulnerabilities (CVEs)
    b) Provide Network Access Control (NAC)
    c) Quarantine high-risk, rogue and infected devices

What is the real cost of a Breach?

Recently, the Ponemon Institute concluded it's 2016 Data Breach report. According to this report (excerpted under fair use of the US Copyright Act, source: http://www.ibm.com/security/data-breach):

> **The cost of data breach sets new record high.** According to this year's benchmark findings, data breaches cost companies an average of $221 per compromised record – of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees.

The total average organizational cost of data breach reaches a new high. In the past 11 years, the most costly organizational breach occurred in 2011, when companies spent an average $7.24 million. In 2013, companies experienced a net decrease in total data breach cost to $5.40 million. This year, the total average cost is $7.01 million.

Measures reveal why the cost of data breach increased. The average total cost of a data breach grew by 7 percent and the average per capita cost rose by 2 percent. Abnormal churn of existing customers increased by 3 percent. In the context of this paper, abnormal churn is defined as a greater than expected loss of customers in the normal course of business. The average size of a data breach (number of records lost or stolen) increased by 5 percent.

Certain industries have higher data breach costs. Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research had a per capita cost well below the overall mean value.

Malicious or criminal attacks continued to be the primary cause of data breach. Fifty percent of incidents involved a malicious or criminal attack, 23 percent of incidents were caused by negligent employees, and 27 percent involved system glitches that included both IT and business process failures.

Malicious attacks were most costly. Companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost of $236, significantly above the mean of $221. In contrast, system glitches or human error as the root cause had per capita costs below the mean ($213 and $197, respectively).

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

The more records lost, the higher the cost of data breach. This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

The more churn, the higher the per capita cost of data breach. Companies that experienced less than 1 percent churn, or loss of existing customers, had an average organizational cost of data breach of $5.4 million and those experiencing churn greater than 4 percent had an average cost of data breach of $12.1 million.

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

Detection and escalation costs are at a record high. These costs include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs increased dramatically from $0.61 million to $0.73 million, suggesting that companies are investing more heavily in these activities.

Notification costs increased slightly. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary mail contacts or email bounce-backs and inbound communication set-up. This year's average notification costs increased slightly from $0.56 million in 2015 to $0.59 million in the present year.

Post data breach costs increased. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. These costs increased from $1.64 million in 2015 to $1.72 million in this year's study.

Lost business costs increased. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The current year's cost of $3.97 million represents an increase from $3.72 million in 2015. The highest level of lost business cost was $4.59 million in 2009.

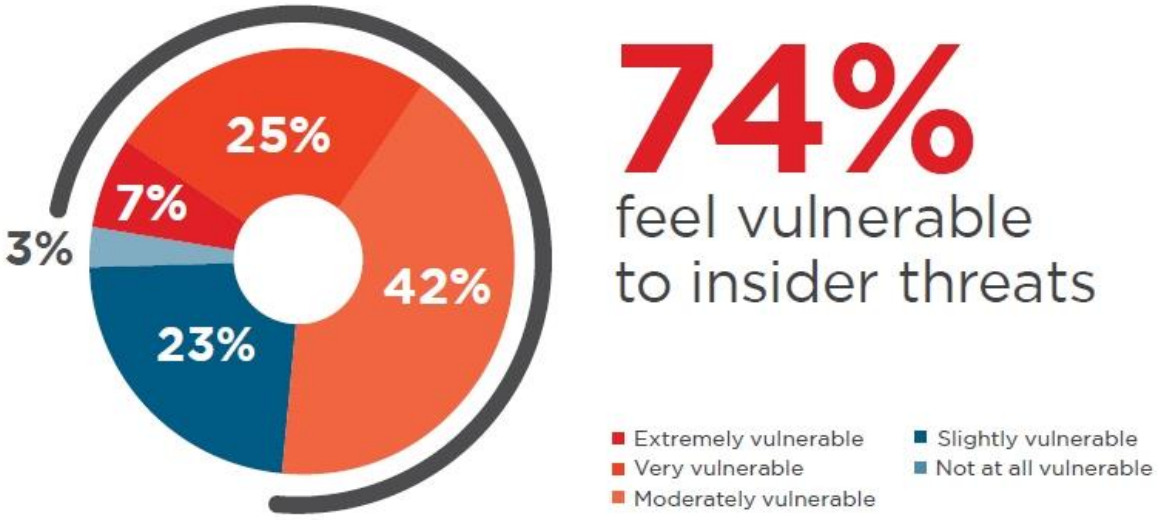
Companies continue to spend more on indirect costs than direct costs. Indirect costs include the time employees spend on data breach notification efforts or investigations of the incident. Direct costs refer to what companies spend to minimize the consequences of a data breach and to assist victims. These costs include engaging forensic experts to help investigate the data breach, hiring a law firm and offering victims identity protection services. This year the indirect costs were $145 and direct costs were $76.

The bottom line is this: Breaches are EXTREMELY costly and may put your organization out of business and you, out of a job. Isn't it time to take an Offensive approach to cyber security? Aren't you tired of reading about breaches in the news, wondering if your organization will be next?

Are Insider Threats Really That Serious?

According to the Insider Threat Report of 2016, by Crowd Research Partners, Seventy-four percent of organizations feel vulnerable to insider threats - a dramatic seven percentage point increase over last year's survey.

Even though only 42 percent of companies feel they have appropriate controls to prevent an insider attack, only three percent of companies feel they are not at all vulnerable to an insider attack.

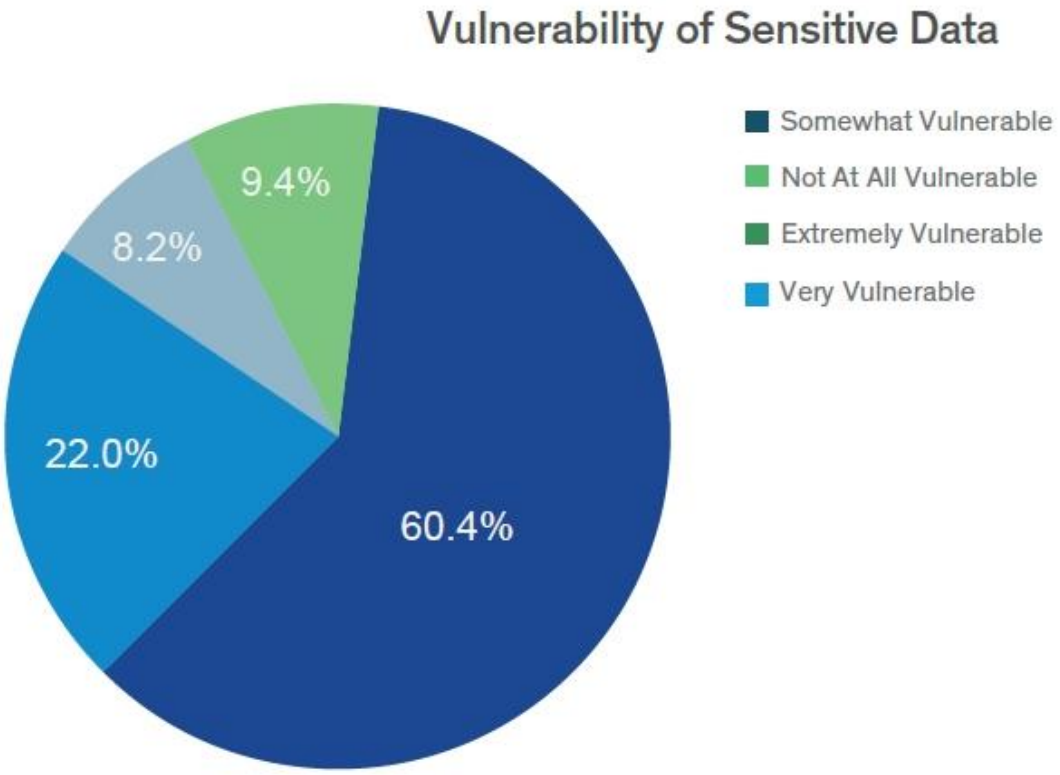


What most organizations don't realize is that most employees have no malicious intent – they just aren't properly trained to handle Spear Phishing, Remote Access Trojans and Ransomware, among other cyber threats. In addition, highly vulnerable systems as well as infected (including mobile, through spyware and creepware apps) systems are wide open doors. Most antivirus software misses at least 50% of the latest malware while firewalls have no intelligence to block the cleaning company from plugging in a rogue laptop at midnight, for example.

In addition, the detection of a breach which usually begins BEHIND the firewall is much more difficult to discover than the traditional breach attempt coming from the outside-in. The main reason is that most organizations have not deployed agentless, non-inline Network Access Control (NAC), have not documented their internally exploitable

Vulnerabilities known as Common Vulnerabilities and Exposures (CVEs) as defined by http://NVD.nist.gov in the National Vulnerability Database, updated very frequently, and have no way of quarantining, nearly instantly, infected, soon to be infected or rogue network assets, behind the corporate firewall. Also, the Bring Your Own Device (BYOD) dilemma has left the corporate 'backdoor' wide open to data leakage through mobile devices loaded with creepware, spyware and very powerful data leakage ports – webcam, Bluetooth, nfc, microphone, keyboard, wifi, 3g/4g, gps, etc.

From the Vormetric 2016 Global Data Threat Report, when it comes to the risk of personally identifiable information (PII) or mission critical confidential data being stolen or at risk, the numbers are astoundingly high:



And, the proof is in the pudding – according to PrivacyRights.org we've seen nearly ONE BILLION PII RECORDS stolen in the USA alone (see http://www.privacyrights.org and click on 'chronology of data breaches').

You'll see most of these breaches are starting to happen on Small to Medium Sized Enterprises (SMEs) more than ever before.

SMEs have become the #1 target of cyber breaches because they are easier targets than those like a Bank of America who has a $400M per year Cyber Security budget and a huge INFOSEC team protecting their networks 7x24x365 and who can weather a major breach, as they manage over $4 TRILLION US DOLLARS.

The only way to get ahead of a breach is to not let it happen and if it does, to instantly, quickly, automatically isolate it and minimize the impact.

So, now that you've seen how costly breaches are and you've also now know my 7 secrets of Offensive Security, let's discuss each one in more detail. Here they are:

1. Demand Executive Support

This may not be easy, however, you will have to get the Board of Directors, the CEO, CFO, CIO, etc., all top level executives to agree that, fiduciarily, the right thing to do to avoid a breach is to have an annual budget, agree that training of all employees is important, that a corporate security policy is a must have and how the corporation will react if and when a breach actually does happen.

Steps involved:

1) Schedule a meeting with key executives (Board Members, CEO, CFO, CIO, etc.) and explain that you want to share a way to dramatically reduce the risk of the corporation suffering a major outage, fines, penalties, lawsuits, business disruption and possibly going out of business. That will get their attention.

2) Present they typical costs of a Breach and why you think your organization is at risk. Try to cover what you think your organization is missing from my 7 Offensive Security Secrets – funding, training, frequently tested backups, corporate security plan, fuel for the backup diesel generator, corporate wide encryption, etc.

   Whatever the infosec gaps and related issues that are on your mind should be presented in an organized and thoughtful fashion.

   If you could sum up the costs in people/time/money that you need vs the cost of a breach, you'll probably find that your requests are 1/10th or less than the cost of a breach.

3) Explain that this is an ongoing process, you'd like to document steps being taken and results on a mutually agreeable frequency and then schedule your first followup meeting with them to present the ongoing risk reducing results.

2. Deploy Continuous Backups and Test Them Regularly

When is the last time you tested a 'restore' of a backup file? When did you most recently backup employee desktops, laptops, servers and other critical infrastructure? While there are numerous and very solid backup products in the market, some even open source (free), there is a smaller list of continuous data protection products that are doing backups in real-time. Continuous data protection (CDP), also called continuous backup or real-time backup, refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves.

Steps involved:

1) Inventory all network attached assets throughout your entire organization – in particular, the operating systems you are running.

2) Find a CDP product that runs on all the operating systems where you value data – laptops, desktops, servers, etc. If they have a client for smartphones, that would be a plus however, at the time of this writing, it's doubtful. If that's the case, look for an additional backup product or consider Google or Apple's hosted offering such as Google+ and the iCloud.

3) Test your backup solution and make sure it can restore properly on a few key test platforms such as windows and linux. If it meets your needs, deploy it corporate-wide.

3. Deploy Corporate-wide Encryption

Encryption is one of the most powerful ways to protect personally identifiable information (PII). There's encryption for data in transit, encryption for entire hard drives, databases and file systems. If you have employees who travel frequently, if there were a way to encrypt their smartphone, tablet, laptop, netbook and notebook hard drives and file systems that would be the best place to encrypt first – in many cases employee traveling equipment are lost or stolen and without encryption, whatever corporate records, data, passwords, VPN client or other confidential information could end up in the hands of criminals or other preying eyes. There are some excellent encryption technologies on the market – some encrypt chat sessions, instant messaging and SMS as well as telephone or voip communications. These are great for data in transit. There are numerous free and open source tools like Stunnel, OpenSSL, OpenSwan and TrueCrypt (v6 or earlier) that will provide you with a high level of encryption. If there's ever a breach either on portable equipment or behind the corporate firewall, you can mitigate data theft risk, if the data that's accessible to the hackers and cyber criminals is encrypted and they don't have the keys.

Steps involved:

1) Inventory all network attached assets throughout your entire organization – in particular, the operating systems, file systems and databases you are running.

2) Find encryption solutions that will protect these operating systems, file systems and databases. You'll probably end up with multiple solutions from a mix of open sources or different vendors. So, you won't end up with a single dashboard to manage all the encryption but even so, it's worth the effort.

3) Test and deploy the encryption across your organization. The biggest headache will be multi-factor authentication and key management so make sure you picked the most manageable solution with the ability to recover keys or reset passwords without losing access to the data.

4. Create a "Living" Corporate Security Document

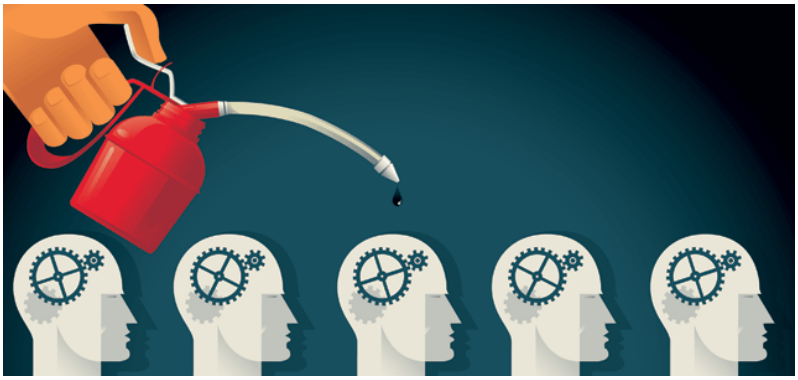
A 'living' corporate security policy is your documentation that states in writing how your organization plans to protect the company's physical and information technology (IT) assets. It's a living document because it's never final – you should be continually updating it based on geographic risk, people risk, physical and network resources risk and other forms of risk that might be changing or evolving over time, affecting your organization. As new threats arrive, such as Ransomware, you'll want a corporate security anti-phishing policy and a policy on how to deal with ransomware, for example. Most corporate security policies include acceptable use, password management, network access control, bring your own device policies, encryption policies and others with descriptions on mitigating risk and how policies are to be enforced. You'll also want to deploy policies that help you prove due care and due diligence in compliance with regulations that affect your organization (FISMA, EU GDPR, GLBA, SOX, HIPAA-HITECH, VISA PCI, etc.).

Steps involved:

1) Review various corporate security models and find one you like – most are inexpensive and even freely available such as ISO27001, found here: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm, ISACA's COBIT, found here: http://www.isaca.org/cobit/pages/default.aspx, or the NIST cybersecurity framework, found here: http://www.nist.gov/cyberframework/.

2) Explain to key executives and employees how important this document and their acceptance is for protecting the organization from regulatory compliance pressures, to maintain compliance and reduce the risk of a breach. Have them look at this one story to see what happens when a regulator (over-reaches) gets involved: http://michaeljdaugherty.com it won't be the breach that puts you out of business, it might actually be a government regulator.

3) Roll it out and update it as necessary. Test the controls in each policy section. For example, test password management as well as backup/restore.



5. Train and Retrain All Employees on Best Practices INFOSEC Policies

So, now you have a great 'living' corporate security policy. Do your fellow employees from the "C" levels down to the receptionist understand these policies? Are they helping you implement them or are they becoming difficult and a hindrance to your documented regulatory compliance and best practices? Of all the policies you're implementing, which one's will most likely cause a breach or data theft, if an employee violates the policy? The most important would be a Bring Your Own Device policy (BYOD) as it's a network asset that you are allowing to cross the bounds, outside of your firewall and then returning, most likely in a different (maybe infected, maybe more insecure) state. Others include ensure devices have the latest patch and application updates, as well as proper configuration and system hardening, to reduce the risk of Common Vulnerabilities and Exposures (CVEs) that get exploited by hackers, cyber criminals and malware. Antivirus software should be up to date but it won't stop the latest exploits – especially Spear Phishing, Remote Access Trojans (RATs) and Ransomware. This requires a better educated employee population who understand that sending and receiving un-encrypted emails is a big risk, emails with attachments and being too trusting to click links and open attachments without verifying the senders' true identities. This leaves them wide open to being socially engineered and victimizing your organization.

Steps involved:

1) Train employees about the risks of BYOD, lack of updated systems, traveling with laptops using weak passwords, no encryption and the biggest risks of being spear phished, then being infected with nearly invisible malware.

2) Schedule these training sessions using statistics, graphics, memes and other tools to make it 'pop' – it should be fun and visual so they will enjoy the learning experience. You could even make it a game. Whatever it takes, get the employees engaged and understanding the value of best practices – stronger passwords, strong encryption, regular backups, safer BYOD, etc.

3) Send out INFOSEC updates. Give out awards. Keep the employees engaged. The more aware they become, the lower the risk of victimization.

6. Manage the Bring Your Own Devices (BYOD) Dilemma

Bring your own device (BYOD) has become pervasive. Most companies are being pressured by their executives for cost reduction and productivity boosting, to allow employees to bring their personally owned devices (laptops, tablets and smartphones) to work. They are asking for privileges to, either behind the firewall over corporate wifi, or over the public internet using 3G/4G or public wifi, to be able to VPN into corporate resources from these traveling devices. There could not be a riskier thing to do, when it comes to corporate security. The main reason is that the state of these devices is ever changing – applications, emoji keyboards, vpn clients and even productivity sinkhole games like Pokemon Go have taken over the mindset of end-users. Most employees have 30-50 unmanaged apps running on these devices and many are freeware given away in return for access to their personally identifiable information – phone identifiers, contacts list, email information, social media passwords, geolocation and much more – turning these devices into fully loaded creep ware and spyware platforms.

Steps involved:

1) Create a 'living' BYOD policy and make sure everyone who is allowed to leverage their own devices agree to the policy.

2) Train them as to the risks inherent in the free apps they already have on their devices. Explain to them that their Emoji Keyboard is probably a keylogger and it should be deleted if it didn't come with the phone from the operating system vendor – Microsoft, Google, Apple or RIM. The same holds true for all of their other free apps. It's time to do a spring cleaning – remove all the unused apps. Evaluate the rest for their affect on privacy and data leakage risk. What hardware ports do they use? Do they really need to access Keyboard, Microphone, Webcam, Bluetooth, Wifi, NFC, 3G/4G, GPS, etc. Does their privacy policy look onerous? If so, convince the employee to find a safer replacement app.

3) Enforce rules through BYOD agent-based software to prevent Data Leakage. Make sure these rules protect the corporation and are enforced during working hours, through geolocation and/or VPN remote access.

7. Deploy and Manage a Breach Prevention Solution

You have a firewall. Check. You have anti-virus. Check. Ok, so now you are about 5% protected. Now is the time to deploy a breach prevention solution because over 95% of breaches happen behind the corporate firewall on systems running the latest antivirus software. Can you tell if a system has a critical vulnerability that is easily exploitable? Do you know if the Cleaning Company is plugging in a rogue device on your network this evening? What about an employee who forgot about your spear-phishing policy and just clicked a link leading to an installation of Locky Ransomware that will probe your corporate network to attempt to encrypt not only the employee desktop but all of your fileservers? How do you get one step ahead of these threats? With a breach prevention solution.

Steps involved:

1) Find a breach prevention solution that you can afford and that you like. There are many new ones on the marketplace today. Some are called internal intrusion prevention devices, others are called anti-malware gateways and anti-phishing email systems but these are all point solutions. You'll need to focus on those that help you do the following three things:

    d) Document and mitigate RISK, especially serious vulnerabilities (CVEs)

    e) Provide Network Access Control (NAC)

    f) Quarantine high-risk, rogue and infected devices

2) Selfish-plug: While we at SnoopWall make NetSHIELD as affordable, cost effective and easy to deploy breach prevention solutions, you could also look into Forescout, Fireeye, IBM and/or a mix of point solutions like Qualys, Rapid7, better managed switches, Cisco's 802.1x NAC solution, etc. Ultimately, it's up to you to find the best tools you can work with to help you find and fix your vulnerabilities, manage access to your network and quarantine rogue and/or infected devices.

SnoopWall's Award Winning, Affordable Breach Prevention Solution:

SnoopWall, Inc. proudly manufactures in the USA, the patented NetSHIELD appliances for intranet breach prevention, shipping them worldwide, (see: https://www.youtube.com/watch?v=fDO3dkOV-1M) receiving numerous awards and the award winning WinSHIELD and MobileSHIELD endpoint data leakage prevention technology based upon AppSHIELD SDK, SnoopWall's patented mobile security toolkit that has already been used to protect hundreds of thousands of financial transactions that take place through mobile banking applications. To learn more about these products and services, visit: https://www.snoopwall.com/products-services/

NetSHIELD™

Third-Party Evaluations & Awards

"Full dynamic access control and auditing of network devices."
- Peter Stephenson, SC Magazine

SC Magazine Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★

SC MAGAZINE RECOMMENDED

Info Security Products Guide GLOBAL EXCELLENCE AWARDS ★★★★★

NETWORK PRODUCTS GUIDE PRODUCT INNOVATION ★★★★★

SC MAGAZINE Top Product 2020

For: Full dynamic access control and auditing of network devices.

Against: None that we found.

Verdict: A solid suite of hardcore NAC products with a clear focus on keeping unauthorized systems and users off the network.

About SnoopWall

SnoopWall is the world's first breach prevention security company delivering a suite of network, mobile and app security products as well as cloud-based services protecting all computing devices from prying eyes and new threats through patented counterveillance cloaking technology. SnoopWall secures mission critical and highly valuable confidential information behind firewalls with our award winning patented NetSHIELD appliances and with WinSHIELD on windows and MobileSHIELD on Google Android and Apple iOS mobile devices with next generation technology that detects and blocks all remote control, eavesdropping and spying. SnoopWall's software products and hardware appliances are all proudly made in the U.S.A. Visit us at http://www.snoopwall.com and follow us on Twitter: @SnoopWallSecure.

About The Author

Gary Miliefsky, fmDHS, CISSP®, CEO, SnoopWall

Gary is the CEO of SnoopWall, Inc. and a co-inventor of the company's innovative breach prevention technologies. He is a cyber-security expert and a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in both Forbes and Fortune Magazines. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). He also assisted the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace as well as the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Previously, Gary has been founder and/or inventor for technologies and corporations sold and licensed to Hexis Cyber, Intel/McAfee, IBM, Computer Associates and BlackBox Corporation. Gary is a member of ISC2.org and is a CISSP®. Email him at ceo@snoopwall.com.

Learn more about SnoopWall's cybersecurity expert CEO at:

http://www.snoopwall.com/media/

For CEO interviews and Press Inquiries Contact:

Brittany Thomas
News & Experts
727-443-7115 Ext: 221
Email: brittany@newsandexperts.com

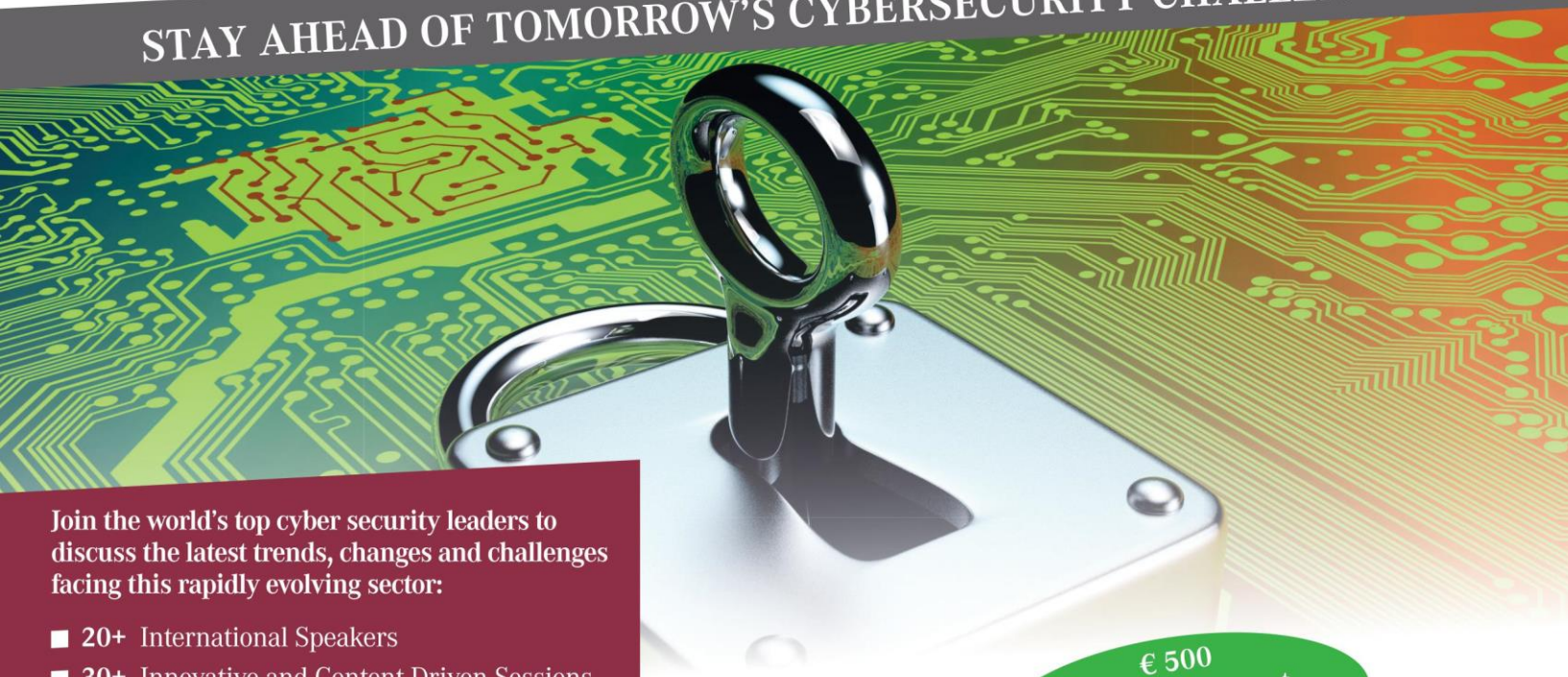
2nd ANNUAL SUMMIT

GLOBAL CYBER SECURITY LEADERS

EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

7th – 8th NOVEMBER, 2016 | STEIGENBERGER AM KANZLERAMT | BERLIN

STAY AHEAD OF TOMORROW'S CYBERSECURITY CHALLENGES!



Join the world's top cyber security leaders to discuss the latest trends, changes and challenges facing this rapidly evolving sector:

- **20+** International Speakers
- **30+** Innovative and Content Driven Sessions
- **30+** Hours of Exclusive Networking

€ 500 Special Discount with code GCSL4CDM

Speakers include:

Alexander Oesterle
Global VP Governance, Risk & Compliance and CSO, **SAP, Germany**

Daniel Selman
Cyber Industry Deputy Head, **UK Ministry of Defence, United Kingdom**

Stephan Gerhager
CISO, **Allianz Deutschland AG, Germany**

Scott Stewart
Vice President of Tactical Analysis, **Stratfor, USA**

Taiye Lambo
CISO, **City of Atlanta, USA**

Volker Kozok
Assistant Branch Chief German MoD, **Bundeswehr, Germany**

Kim B. Larsen
CSO, **Huawei Technologies, Denmark**

Arieh Shalem
CISO, **Orange Telecommunication, Israel**

Premium Partner

Warth & Klein Grant Thornton
An instinct for growth™

Promoters

EY Building a better working world

ThreatBook

Hosted by

MANAGEMENTCIRCLE®

Official Part of

Global Leaders Summit Series
EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

www.cybersecurity-leaders.com

Ensure Your Data is Not Taken Hostage: Ransomware Remediation Strategies

Raj Samani, VP & CTO, EMEA, Intel Security

After slowing slightly in mid-2015, ransomware has overall regained its rapid growth rate. According to the *June 2016 McAfee Labs Threats Report*, total ransomware grew 116% year-over-year for the period ending March 31. Total ransomware rose 26% from Q4 2015 to Q1 2016 as lucrative returns continued to draw relatively low-skilled criminals.

An October 2015 Cyber Threat Alliance analysis of the CryptoWall V3 ransomware hinted at the financial scale of such campaigns. The researchers linked just one campaign's operations to $325 million in victims' ransom payments.

This spurt in Ransomware attacks can be attributed to three key reasons. The first driver is the syndication of the activity into ransom as a service with offers of revenue sharing to operatives facing the target recipients.

The second driver is the development of polymorphism in ransomware generating a unique threat signature for each attack. And the third driver is the increasing sophistication within the malware, widening the scope of damages.

With Middle East organizations becoming a target for Ransomware attacks, it is incumbent on the C-suite to take action and ensure that their data and organizations are not held ransom.

Remediation Strategies for Each Stage

Ransomware attacks occur in five stages – distribution, infection, communication, encryption and demand. So it is only logical that there should be prevention and remediation strategies for each of these stages.

Distribution Stage

Build a "human firewall": The biggest threat is users who let the ransomware on their endpoints. People are the weakest link. Organizations need to make sure that all employees from the CEO down, understand both how ransomware works as well as the ramifications of an attack

Stop ransomware before the endpoint: The most-proactive method of protecting a network from ransomware attack (other than the human firewall) is to keep ransomware from reaching the endpoint in the first place. Consider a web-filtering technology

Apply all current operating system and application patches: Many ransomware strategies take advantage of vulnerabilities in the operating system or in applications to infect an endpoint. Having the latest operating system and application versions and patches will reduce the attack surface to a minimum

Spam filtering and web gateway filtering: Again, the ideal approach is to keep ransomware off the network and the endpoint. Spam filtering and web gateway filtering are great ways to stop ransomware that tries to reach the endpoint through malicious IPs, URLs, and email spam

Allow only whitelisted items to execute: Use an "application control" method that offers centrally administered whitelisting to block unauthorized executables on servers, corporate desktops, and fixed-function devices, thus dramatically reducing the attack surface for most ransomware

Limit privileges for unknown processes: This can be done easily by writing rules for host intrusion prevention systems or access protection rules

Infection Stage

Don't turn on macros unless you know what's happening: In general, do not enable macros in documents received via email. Notice that Microsoft Office turns off auto-execution of macros for Office documents by default. Office macros are a popular way for ransomware to infect your machine, so if a document "asks" you to enable macros, don't do it

Make yourself "weaker" when working: Don't give yourself more login power than you need. If you allow yourself administrator rights during normal usage, consider restricting this.

Surfing the web, opening applications and documents, and generally doing a lot of work while logged in with administrative rights is very dangerous.

If you get hit with malware while you have fewer rights, you will reduce your risk because malware will also execute with fewer rights, which will reduce the threat's attack surface

Use access protection rules on software installs: Write access control rules against targeted file extensions that deny writes by unapproved applications. This complements host intrusion prevention systems rules with a similar strategy

Use sandboxing for suspicious processes: If a process is flagged as suspicious (due to low age and prevalence, for example), that process should be sent to a security sandboxing appliance for further study

Block "unapproved" processes from changing files: Block these by writing rules for host intrusion prevention systems or access protection

Communication Stage

Firewall rules can block known malicious domains: Writing rules to block malicious domains is a standard capability of network firewalls

Proxy/gateway scanner signatures for known traffic: For those with proxy and gateway appliances, these technologies can be configured to scan for known ransomware control server traffic and block it. Most ransomware cannot continue operations if it cannot retrieve the public encryption key needed for asymmetric encryption

Encryption Stage

Back-up and restore files locally: By creating a storage volume and running archival differential-based file backups to that storage volume, remediation is as easy as removing the ransomware, going back in time with the backup to a point before the ransomware affected the files, and restoring all the affected files.

This can be done today by network administrators who could either use external storage volumes with a good archival backup utility or partition a local drive and run the backup utility against that

Limit shared file activities: Many ransomware variants will look for access to files on storage other than the boot volume—such as file servers, additional volumes, etc.—and will encrypt everything they can find to inflict maximum damage. Consider limiting operations allowed on shared volumes

Ransom Demand Stage

Restore from backup, keep a recent backup offsite and "air gapped": Store a set of multiple, complete backups and assume an attack. An "air-gapped" backup is not connected to the computer or the network anywhere. (For an individual this could mean back up to an external hard drive.

When the backup is done, unplug the drive and keep it in a drawer, away from any computers. That way ransomware cannot detect the backup and damage it.)

Consider using a "bare metal backup" utility, which not only backs up your user files, but also lets you erase all storage volumes (in case the machine is stolen) and get you back to a usable state with all your applications and data restored

Ensuring your organization's precious data is not ripe for the taking is a daunting task, especially with the steady rise of ransomware as an attack vector.

By adopting a planned approach involving both end users and IT administrators, and implementing integrated security solutions that protect, detect and correct, businesses can avoid the unplanned downtimes and losses associated with such malware attacks.

About the Author

Raj Samani is an active member of the Information Security industry, through involvement with numerous initiatives to improve the awareness and application of security in business and society.

He is currently working as the EMEA Chief Technical Officer for Intel Security, having previously worked as the Chief Information Security Officer for a large public sector organisation in the UK.

He was inducted into the Infosecurity Europe Hall of Fame (2012), won the Virus Bulletin Péter Ször Award for the paper/investigation he co-authored on the takedown of the Beebone Botnet, and was named in the UK's top 50 data leaders and influencers by Information Age.

He previously worked across numerous public sector organisations, in many cyber security and research orientated working groups across Europe. He is also the author of Syngress books 'Applied Cyber Security and the Smart Grid', "CSA Guide to Cloud Computing", and technical editor of "Industrial Network Security (vol2)" and "Cyber Security for decision makers".

In addition, Raj is currently the Cloud Security Alliance's Chief Innovation Officer and previously served as Vice President for Communications in the ISSA UK Chapter where he presided over the award of Chapter Communications Programme of the Year 2008 and 2009.

He is also Special Advisor for the European CyberCrime Centre, also on the advisory council for the Infosecurity Europe show, Infosecurity Magazine, and expert on both searchsecurity.co.uk, and Infosec portal, and regular columnist on Help Net Security.

He has had numerous security papers published, and regularly appears on television commenting on computer security issues.

ATTENTION: A MUST ATTEND EVENT FOR
ALL SENIOR LEVEL CYBER SECURITY EXECUTIVES

DC Metro • June 30 | Chicago • August 25 | New York • September 21

CYBER SECURITY SUMMIT

Attend the Cyber Security Summit

Connecting Senior Level Executives with the world's leading Cyber Solution Providers and Thought Leaders

Register at CyberSummitUSA.com using Promo Code: CDM2016 for 50% OFF Full Summit Passes

Thought Leaders, Speakers & Advisors Include

Ronald Yearwood
Section Chief of Cyber Ops III
FBI Cyber Division

Ralph Kahn
VP of Federal
Tanium

David Cass
CISO
IBM

Paul Fletcher
Cyber Security Evangelist
Alert Logic

Elisabeth Maida
Co-Founder & CTO
Uplevel Security

Todd Helfrich
VP, Federal
Anomali

Curtis Dukes
Director Info. Assurance
The NSA

Partial List of Solution Providers

ALERTLOGIC · ANOMALI · BALABIT · BLUE COAT · BUFFERZONE · Centrify · CENTRIPETAL NETWORKS · CenturyLink · CYLANCE · DARKTRACE · dashlane · deepinstinct · mazzanti technologies · esentire · iboss CYBERSECURITY · Infoblox · intel Security · NATION-E · NSS LABS · RE-SEC · red canary · SEPIO SYSTEMS · SiteLock · passcode · TANIUM · THREATQUOTIENT · UPLEVEL · US CYBER VAULT · VECTRA · Vormetric Data Security · WatchGuard · Zerto · And More

To Exhibit Contact Bradford Rand at **212.655.4505 ext 223** or **BRand@TechExpoUSA.com**

www.CyberSummitUSA.com

U.S. Government Announces Framework for Responding to Critical Infrastructure Cyber Incidents

What Operators of Critical Infrastructure Need to Know About PPD-41

By David Navetta, Boris Segalis, Mia Havel and Kris Kleiner, Norton Rose Fulbright US LLP

On July 26, 2016, the White House issued the United States Cyber Incident Coordination Directive (Presidential Policy Directive PPD-41, including an Annex).

The Directive sets forth the principles governing the Federal Government's response to cyber incidents, including incidents affecting private entities that are part of U.S. critical infrastructure.

The Directive triggers a significant Federal Government role and establishes a framework for its response to "**significant cyber incidents**" in particular and is designed to improve coordination between government agencies and to clarify inter-departmental involvement in response to a cyber incident.

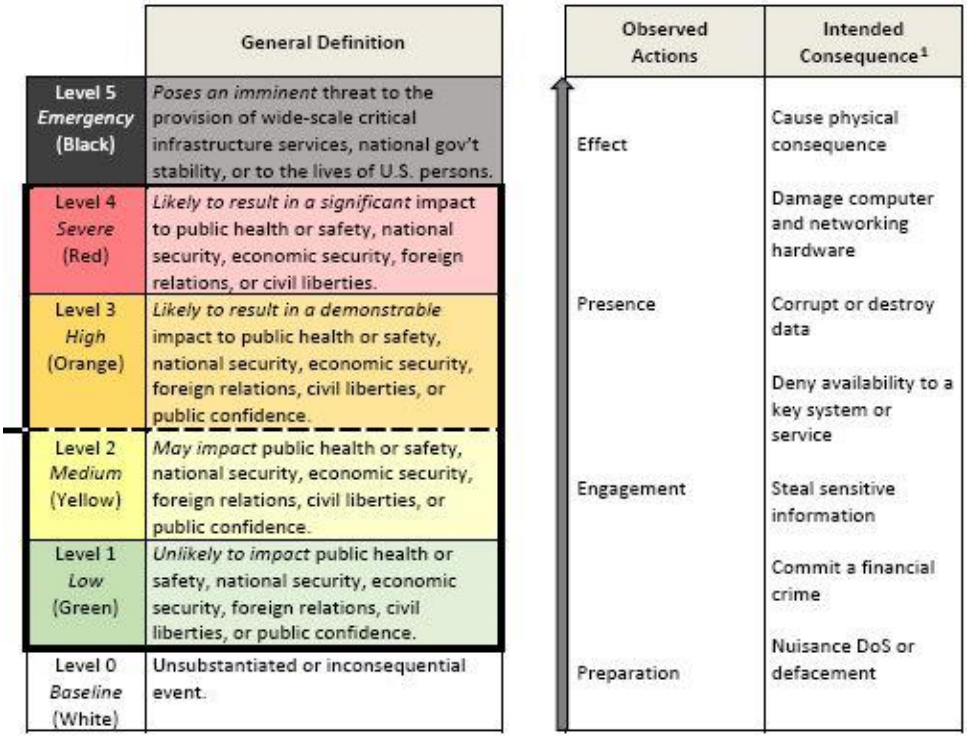
Key Elements of PPD-41

PPD-41 makes a distinction between a "**cyber incident**," which is defined as "[a]n event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon, and a "**significant cyber incident**," which is defined as "[a] cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

In conjunction with these definitions, the Directive includes a Cyber Incident Severity Schema, which further categorizes the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests:

Under this schema, a threat of Level 3 or higher constitutes a "significant cyber incident."

A "cyber incident" will not typically trigger federal government involvement beyond "coordinated efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure" through the relevant sector-specific agency ("SSA").



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

[1] In addition to characterizing the observed activity, one must consider the scope and scale of the incident when applying the general definitions to arrive at a severity level.

Conversely, for "significant cyber incidents," the Directive establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response to the incident. Specifically, PPD-41 assigns lead response roles for:

- Investigation/Information Sharing: The Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, will lead the "threat response activities," which include investigative activity, providing attribution, linking related incidents, identifying threat pursuit and disruption opportunities, and facilitating information sharing and operational coordination with asset response.

- Asset Protection: The Department of Homeland Security will lead "asset response activities," which include furnishing technical assistance to affected entities, mitigating vulnerabilities, reducing impacts of cyber incidents; assessing potential risks to the sector or region; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

- Intelligence Support: The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, will lead "intelligence support," which includes building situational threat awareness and sharing related intelligence; the

analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

For significant cyber incidents, the Federal Government may take these steps even if the targeted entity is in the private sector.

The incident response will be coordinated through a Cyber Unified Coordination Group or Cyber UCG, normally consisting of the federal lead agencies identified above, the relevant sector-specific agency ("SSA") that typically serves as the primary regulator for the impacted entity, and private sector entities.

Additionally, the Annex imposes deadlines on federal agencies to complete various action items within the next three to six months to facilitate the implementation of the Directive, many of which require that the agencies consult with industry stakeholders.

For example, federal agencies are required to develop sector-specific procedures for incident response coordination and to develop a national incident response plan for critical infrastructure.

Impact on Critical Infrastructure Operators in the Private Sector

Because many of the requirements of PPD-41 will have to be implemented in the next several months, the full impact of the Directive remains unclear. However, we anticipate the following impact on private sector companies involved with critical infrastructure:

Internal incident response plans will need to be updated

We expect that the development of sector-specific incident response procedures to require private entities to take steps to embed coordination with SSAs into the entities' incident response plans.

Increased government involvement with cyber incidents

Because PPD-41 establishes clear responsibilities among federal agencies, we expect government involvement in the investigation, response, and intelligence gathering activities related to cyber incidents may be more extensive than it has been in the past.

This may particularly be the case when the government designates a cybersecurity event as "significant" and thus assembles a Cyber USG to support the incident response. We also expect agencies to better articulate the types of events that they would view as "significant."

One potential benefit to private sector companies is that PPD-41 may clarify expectations and lead to fewer regulator "turf battles" in the wake of an incident. To some extent, government

involvement following a cyber-security incident is to be expected, particularly for major incidents in highly regulated industries.

Because the Directive provides structure and parameters around agency roles and responsibilities, it not only helps set expectations about what an expect and from which agency when the government gets involved, but it may also reduce duplication of effort and overlapping requests from multiple federal agencies.

Notably, the Directive emphasizes the need for the government's involvement in incident response to be efficient and constructive, directing that the government response should take into account the "need to return to normal operations as quickly as possible" when engaging an entity in the wake of an incident.

Increased publicity following cyber incidents

The private sector should expect that the Federal Government's involvement may lead to increased publicity for cyber incidents.

While PPD-41 states that the government will "safeguard details of the incident" and "sensitive private sector information," it makes clear that the government need only determine that a "significant Federal Government interest is served" by issuing a public statement about the incident before making such a statement.

Although the Directive suggests that agencies "generally will defer to affected entities in notifying other affected private sector entities and the public" and will "coordinate their approach with the affected entities to the extent possible," organizations must remain conscious that controlling messaging and publicity following a cyber incident will be complicated by government involvement, and the Directive will do little to curtail regulators in this regard.

For public companies, this may have additional implications related to SEC-required disclosures.

Opportunity to Participate in the Development of Procedures and Plans

Finally, the Annex contains specific provisions calling for the SSAs to "coordinate with critical infrastructure owners and operators to synchronize sector-specific planning consistent with this directive."

Likewise, the national incident response plan is to be "developed in consultation with . . . owners and operators of critical infrastructure, and other appropriate entities and individuals."

This gives private sector players an opportunity to have a voice in the government's development of incident response procedures for their industry.

About The Authors

David Navetta is a US co-chair of Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group. David focuses on technology, privacy, information security and intellectual property law.

His work ranges from compliance and transactional work to breach notification, regulatory response and litigation. David has helped hundreds of companies across multiple industries prepare for and respond to data security breaches.

Boris Segalis is a US co-chair of Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group and has practice exclusively in this area since 2007.

Boris advises clients on data protection, privacy and cybersecurity issues arising in the context of compliance and business strategy, technology transactions, breach preparedness and response, disputes and regulatory investigations, and legislative and regulatory strategy.

He represents clients across industries, from Fortune 100 global organizations to emerging technology and new media companies.

Mia Havel and Kris Kleiner are associates in Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group.

Both Mia and Kris regularly advise clients on best practices as well as compliance with state and federal privacy and cybersecurity regulations and have experience assisting various clients operating in multiple industries in identifying, remediating, and responding to data privacy incidents.

David, Boris, Mia and Kris can be reached at David.Navetta@nortonrosefulbright.com, Boris.Segalis@nortonrosefulbright.com, Mia.Havel@nortonrosefulbright.com, and Kris.Kleiner@nortonrosefulbright.com, or at our company website http://www.nortonrosefulbright.com.

The Case Study: The Stuxnet Operation

By Milica Djekic

The Stuxnet is a malicious computer worm which is believed to be the part of the US-Israeli secret project that got the task to destroy the Iranian nuclear program. The entire case occurred in 2010 and right here we would try to explain what happened then.

Through this article, we intend to talk a bit more about this sophisticated cyber weapon and discuss how it was possible to conduct such an operation.

As Stuxnet was the advanced persistent threat – it's clear why it could go through that defense, but how the entire campaign got conducted is a sort of complicated question and we are ready to provide such an answer right here.

Phase 1: The data collection before any attack occurred

Through this review, we want to discuss our perspectives how the Stuxnet operation could occur and present a new insight into this well-known sabotage. Many resources would suggest that the computers with the entire network got infected through a USB stick, which could get accurate. On the other hand, it's not necessarily needed to provide a physical access to such an infected removable device to your critical asset.

The infection of the USB device could occur inside the facilities simply using that stick with some globally connected computer that could get the target of, say, state-sponsored hacker's attacks. The entire attack could pass as invisible for the reason the Stuxnet got unknown to any computer's defense system of that time. In addition, we should never underestimate the capacities of professional security equipment being used by state-sponsored hackers – but we would not discuss anything of that through this effort.

Many reports would indicate that the reason to such sabotage would be that removable device, so we would try to analyze how it was possible to happen under those circumstances. It's more like leading the investigation using the findings you can collect at the first glance.

Right here, we would suggest that the intelligence community would obtain the information about that nuclear program being conducted for the terrorist purposes through its hard work. Once the intelligence community obtained the details about geo-location of those facilities being somewhere in Iran – they would put the entire location under the exposure.

It's not necessary to monitor such a project from the close, but rather remotely using highly sophisticated technology. The good way to discover such an asset is to follow someone being

correlated with the terrorism and monitoring his communications find those facilities. The modern defense technology would offer you the real-time scanning of some terrain using antenna systems which can cover miles and miles throwing their stream of waves.

Those systems could identify an electrical signal anywhere within a range. We would suggest that such a technology could get used for discovering the Iranian nuclear facilities.

From that perspective, it's clear that the defense forces would see literally everything happening within those objects from the outside.

It's possible that the Iranian experts would use some measures of protection in sense of intelligent computer's network infrastructure, but they would make a mistake using the USB sticks for their data transfer. It would appear that the Iranians would get aware of that the project's computers and networks should not get exposed to the internet for the reason of hacker's attacks.

On the other hand, they could use some computers with the internet connection for communications purposes. Also, those computers could get helpful for finding and doing storage of web resources as well as transfer of the project documentation being sent through the e-mail or any other communication means.

The defense community would observe their routine very carefully and probably notice that the Iranian weakness got that they would do that data transfer using the removable device. In other words, computers being used for a project development would not get the internet connection, while the rest would get used for a communication – so they would get opened to the web.

The skillful intelligence work would offer those findings and the rest of the job belongs to the strategists who would decide how to level down this threatening activity.

Phase 2: The strategic preparation of operation

Once the defense community identified the weakness in the Iranian nuclear program and such a weakness got their data transfer, they decided to create the advanced persistent threat that would cause the malfunction of their Siemens PLC industrial computers.

We believe that a team of skillful code's developers could research how those controllers work and create a malware for the purposes of their sabotage within some reasonable period of time.

So, the situation was as follows – you got all computers inside being covered, the intelligence community got familiar with the Iranian routine and finally, highly sophisticated cyber weapon got ready for its use.

Next, all that happened is the defense forces carefully chose the moment to insert their secret weapon into the enemy's communication computers knowing they would make a mistake doing a data transfer using some removable devices.

The rest got the history!

Phase 3: The Stuxnet attack being conducted

After conducting the Stuxnet attack – the Iranian nuclear program got sent more than a decade back to the past and the world got saved from one more threat to the civilization.

The fact is that many people worldwide would report then that their Siemens PLC systems got disabled for some reason.

The later on, people would correlate such an occurrence with the Stuxnet diversion and today it would get well-known that some countries in the world would suffer the side effects of this operation.

Phase 4: The consequences of that attack

The consequences of such an attack would be that the risk coming from one more terroristic threat got removed with some side effects to the rest of the world that would face on the Stuxnet worm during that period of time. In total, the great job has been done!

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.


www.isaffuari.com
20TH
ISAF
ISAF
IT SECURITY
5TH INTERNATIONAL
INFORMATION &
NETWORK SECURITY
EXHIBITION
ISAF
SMART HOME
5TH INTERNATIONAL
SMART BUILDINGS &
BUILDING AUTOMATION
EXHIBITION
ISAF
SECURITY
20TH INTERNATIONAL
SECURITY & RFID
EXHIBITION
"smart solutions"
SEPTEMBER 29TH-OCTOBER 2ND 2016
İstanbul Expo Center (İFM) - TURKIYE
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr | Tel: +90 212 503 32 32 | marmara@marmarafuar.com.tr
This Fair is organized with the audit of TOBB
(The Union of Chambers and Commodity Exchanges of Turkey) in accordance with the Law No 5174
KOSGEB

Is Your Home Security System Crackable and Outdated?

Burglars are getting smarter. Outwit criminals by boosting your home security system with the latest technologies and techniques. Here are tips to help you solve top security concerns.

by Philip Masterson, Security Advocate, AlarmDefense.com

There was a time when homeowners would simply install steel fences and barbed wires or get canine guards to protect their family and properties. As criminal elements become smarter, the need for better home security has also increased.

A recent study reported that rising security concerns are behind the strong outlook for the home security market. According to researchers, the global home security market will grow at a rate of above 13% between 2015 and 2019. Vendors are boosting investments in research and development (R&D), particularly in introducing new innovations in smart home security systems.

A BBC experiment, however, raises red flags in using smart gadgets, collectively known as the Internet of Things (IoT). “The IoT promises to let stuff, devices and gadgets connect in the same way to both other hardware and us,” writes BBC correspondent Mark Ward.

While these smart gadgets offer convenience and additional protection, many have been proven to be vulnerable and risky.

Check out the following list of guidelines on how to know if your home security system is crackable and outdated.

Photo Courtesy of Unsplash via Pixabay

Are you using a wireless home security system with encrypted signals?

Two security researchers warn that most wireless alarm systems in the market today rely on radio frequency signals that are vulnerable to breaches. These systems are unable to encrypt or authenticate the signals, making it easy for intruders to intercept data and control entryways within a property.

Burglars can simply find the frequencies your home security devices broadcast on (manufacturers are required to list these frequencies), acquire a jamming equipment and begin deciphering commands to control your home security system.

Solutions:

There are wireless security providers that use algorithms capable of detecting radio frequency interference due to jamming attacks. The system notifies the homeowner about the hacking via push alert. An anti-jammer program may be installed in your smartphone.

You may also install a home security system with encrypted signals to bar external sources.

Regardless of the countermeasure you choose, always remember to secure the password on your devices. Change the default password and choose a unique one that is not easily guessed.

Photo Courtesy of kropekk_pl via Pixabay

Do you regularly check the IP history of your surveillance system?

A team of security researchers recently discovered that 18 brands of security cameras are susceptible to hacking, allowing criminals to watch, copy and alter video data. Robbers can even turn off these surveillance cameras before entering a house.

Solutions:

Check whether your device is operating through the networking system UPnP. According to researchers from the NCC Group, this widely-used system is highly vulnerable to attacks. Several vendors have started turning off UPnP by default in their devices.

Regularly monitor the IP history of your security system to detect any unidentified or unknown IP address.

Security experts also recommend purchasing brand new surveillance cameras because used ones may have implanted hacking devices. Be on the safe side: avoid crackable home security equipment by getting new and reliable devices.

Photo Courtesy of geralt via Pixabay

Do you always keep your systems updated?

Sophisticated criminals are knowledgeable, well-equipped and creative. Dr. Claire Nee of the Department of Psychology at the University of Portsmouth, said: “The thing is, you have to be innovative over time because burglars will get used to whatever you do.”

Solutions:

Update your home security software as often as possible to help counter new threats. It is also advisable to consult security experts about upgrades to enhance performance and add new features. Set a routine check-up with professionals once a year.

Another novel strategy to address crackable and outdated home security systems is to build a sustainable home. A sustainable home is one equipped with a smart home security system that can be customized to match the homeowner’s unique needs.

This innovation not only provides the latest in home automation, but also offers eco-friendly equipment.

It need not be said that security plays a huge part in our ability to function as contributing members of society.

To feel safe is simply not a luxury, but something that is integral to our lives, and to have our efforts to keep ourselves, our families, and our property safe be compromised cannot be ignored.

We are compelled to act--to take the necessary steps to reestablish our security and continue to re-enforce those measures. In this light, we continue the tradition of the man who created the first door to keep intruders out of his cave.

Throughout the years, mankind has continuously developed new innovations to stay safe against ever-evolving means to cause them harm. Safety is a legacy we impart upon our loved ones.

About The Author

Philip Masterson is the Owner and Editor of the blog AlarmDefense.com. He is a Market specialist, Researcher, Security Advocate and a Freelance Writer. He have written a range of topics including home and community security, technology, environment, world market and world businesses. Philip Masterson can be reached online at Twitter, Google+, Facebook and at his own website www.alarmdefense.com

CAN YOU **SURVIVE** THE **DIGITAL** TRANSFORMATION?

North Africa Banking Technology 2016 Exhibition

8-9 November 2016
Cairo International Convention Centre

COMPLIMENTARY ACCESS FOR DOMESTIC AND INTERNATIONAL BANKS

6 STREAMS

40+ SPEAKERS

50+ EXHIBITORS

RETAIL BANKING | CORPORATE & INVESTMENT | TRADING | ARCHITECTURE | COMPLIANCE & FINANCIAL CRIME | RISK

WWW.NORTHAFRICABANKING.COM

Sponsors:

Infosys® Finacle

wacom BUSINESS SOLUTIONS

Media Partner:

DIGITAL FORENSICS / MAGAZINE

For more information contact:
Kaleesha Rajamantri
+44 207 111 1615
kaleeshar@irn-international.com

Organised by:

irn International Research Networks

From the Smart Perimeter to the Smart Guard:

Why It's Critical to Understand the Paradigm Shift in Data Security

By: Tom Gilheany, product manager, CISSP, Cisco Systems

Historically, perimeter defense was the gold standard in data security. Guard the perimeter, and you've secured the system. However, in today's landscape, the proverbial "building the castle" is not enough. Cyber criminals are no longer just clawing at the front door—they're also chipping away at bricks, digging tunnels under walls, and sending in Trojan horses.

And that's not to mention the huge number of potential insider threats—including those that are unintentional.

A modern approach—one that goes far beyond simple architecture and perimeter controls—requires an additional focus on security operations.

With the rapid transformation of the security landscape, it's easy for organizations to be concerned that new threats will require a complete overhaul of existing security technology. Not so. Today's threat landscape requires a combination of the old and new.

Adding security operations as a new second layer allows companies to actively and continuously monitor threats, as opposed to using a set-it-and-forget-it approach and hoping for the best.

Protecting an organization today requires a multifaceted strategy that leverages evolving technologies such as Internet of Things, Big Data, and analytics. In addition to external defense, companies require guards that can monitor, detect, and respond to threats across the entire network in real time.

Hardened Walls Must Pair with Smart Guards

Analytics and Big Data capabilities are a necessary part of today's cyber defense. Using the entire network as a sensor allows users to spot the needles in the haystack and hone in on the malicious activity that must be shut down. This is truly a game-changing approach, a stark contrast from the old time-consuming and imperfect ways of manually sifting through alarms.

Today, the ability to program an analytics engine delivers exactly the security data an organization is looking for, and it permits admins to use a triaged approach to gain actionable intelligence.

This pervasive level of network visibility available with today's technology is critical in protecting against threats and is a core element in today's cybersecurity arsenal.

Implementing this shift in defense tactics requires new skill sets. The industry is looking for workers with the skills required to monitor and analyze threat intelligence from across the network.

As a result, security teams today must include more than just those focused on infrastructure. To capitalize on technology that enables network visibility, security staff must have knowledge of what normal network activity looks like, and they must be able to spot anything that deviates from it.

The ability to separate out normal behavior from abnormal gives security teams the advantage of designing defense systems that know what to beware of. The era of the static IT guy who enters various rules into a set-it-and-forget-it system is over.

The Smart Guard Is a Familiar Guard

As an example of that shift, let's compare two types of security guards. One is a longstanding employee of the company, while the other is a temp.

The first security guard knows the owner, knows how the building's dimensions have changed over the years, and knows who the delivery guys and the employees are.

He is familiar enough with the property and its people that he knows instantly when something is out of place or when it doesn't look right.

Importantly, he is a known and trusted entity to those who work at the office. When employees see things that don't look right ("That car tailgated me into the parking lot, and the driver didn't use an access card"), they share that information with the guard, who uses it to perform a check.

Contrast that scenario with that of the security guard working as a temp. He is more likely to be unfamiliar with the property, to perform only cursory checks of the property based on a map layout (which may be outdated), and to lack the relationships with both the office staff and the property itself to have the insight necessary to notice when something is out of place.

For Best Defense, Plug into the People

To properly secure today's organization, security teams must be plugged into its people in addition to the network. The ability to pull actionable data from the network is critical, but security teams must be an active part of the business as well.

By engaging with the business, the security team gains the human intelligence that reduces risk and adds context into whether something is appropriate or suspicious.

The goal is to earn the trust and partnership of the business units so they can work together to secure the organization.

Otherwise, the security team runs the risk of being isolated and perceived as a parking ticket collector, popping up simply to tell colleagues when they're doing something wrong.

This does not motivate the business units from proactively reaching out to the security team with information, and it suppresses the "if you see something, say something" approach that is holistic to security.

Ultimately, the security team must communicate with everyone because security truly is everyone's job.

The Future Requires a Two-Pronged Approach

It will always be necessary for organizations to protect their infrastructure with hardened security.

Yet with the advent of technologies such as cloud, IoT, automation, and network programmability, it is absolutely critical that security be embedded in the fabric and information flow of an organization.

Security staffs today require engineers with the skills and awareness to design, deploy, and manage an operations approach to security.

By combining fortified walls with alert guards throughout the infrastructure, organizations can have a two-pronged approach to protecting their most sensitive data.

About the Author

Tom Gilheany, product manager, CISSP, Cisco Systems

INDONESIA EDITION

ANALYTICS LEADERS SUMMIT 2016

PREDICTING CUSTOMER BEHAVIOUR THROUGH ANALYTICS

19 - 21 OCTOBER 2016 | KEMPINSKI HOTEL JAKARTA, INDONESIA

LISTEN TO THE INDUSTRY EXPERTS

ANALYTICAL PROFESSIONALS ATTENDEES

A 2-DAYS CONFERENCE PLUS A 1-DAY WORKSHOP ON MACHINE LEARNING

ORGANISED BY:

ENIGMA CG
CONSULTING GROUP

3 EASY WAY TO REGISTER

Give us a call at +6032181 7111 ❶

Drop your enquiry to Soraya Sohaimi | soraya@enigma-cg.com ❷

Enquire online at www.enigma-conferences.com /analytics-leaders-summit-in-indonesia ❸

Turning the Tables on Cyber Fraud

By Robert Capps, vice president of business development, NuData Security

The Identity Theft Resource Center reports that so far this year, 572 data breaches have taken place, exposing approximately 13.5 million records. This, despite all the heightened security measures, both internal and external, that organizations have deployed to keep their data safe. At the same time, consumers claim to be concerned about keeping their data safe online but continue to employ unsafe practices such as using the same easy password for multiple accounts and sharing account information with friends and family.

These realities make cybersecurity seem like a pipe dream – but it's far too important to give up on. However, there is a way for organizations to grapple with these twin challenges and still protect their entity and their customers – because ultimately, it's all about the data. As long as it's valuable, it will be stolen. Efforts to devalue data will be the most impactful actions an organization can take to reduce the number, scope and impact of breaches. So how is this accomplished? Read on.

The Never-Ending Battle

Trying to control what happens to data once it has been stolen is like trying to herd cats.

In addition, cybercriminals have numerous ways to attack – and they keep finding more. It's similar to physical crime or terrorism in that way. It's not feasible to protect a soccer stadium, for example, against all possible attack vectors—from every entrance, from the sky, from underground—let alone means of attack that security teams haven't thought of yet.

For these reasons, it's a never-ending, seemingly pitched battle to keep data secure.

The fact is that every time we get it wrong, something bad happens. Sometimes very bad, as in stock-plummeting, customer-fleeing, company-destroying bad.

Becoming Proactive

To lower the odds of getting data security wrong, organizations must create a security culture that seeps into every aspect of doing business. Education is key – the mindset has to change, not just the product. This requires a proactive approach versus a reactive one.

What does this look like in practical terms? Whereas perimeter and infrastructure defenses tend to be reactive, being proactive means observing consumer behavior with much higher fidelity. Traditionally, analysis has tended to be rather superficial. To truly understand and know the user, you need to look deeper. This includes looking for signals you wouldn't normally look for—how fast someone types, how hard they hit the keys, how a user interacts with a website, etc.—the types of signals that are often ignored.

When these signals are combined, they created a distinctive behavior-based user profile that is far more detailed and reliable than standards like passwords and usernames. Knowing a consumer's true behavior transcends reliance on static identities.

Making User Data Useless

User profiles based on distinctive behaviors devalue data. How? Bad actors can't emulate behaviors with enough fidelity to truly take control of a user's identity if the right signals are in place. The focus changes from the user's username, password and perhaps location or secret question to his or her unique identifying behaviors. Deriving identification from measuring these behavioral indicators is so powerful because authenticators can't be replicated.

Malicious actors can't make use of the data they have stolen or acquired on the dark web because they don't have the unique behavioral profiles that correspond to the data.

It's no longer merely an issue of plugging stolen data into a login screen and taking over an account or completing fraudulent transactions; fraudsters would have to exactly mimic every behavior in the profile – an impossible task.

In this way, consumers' personal data is useless to criminals. Why go to the trouble of stealing something you can't benefit from? The incentive for fraudsters to steal this kind of data is zero. In other words, the data has been devalued.

Restoring Confidence

Cyber thieves are stunning in their ingenuity and flexibility, but they're also inherently lazy. They tend to take the path of least resistance as well and nab the loot that's easiest to steal and offers the biggest pay-off. If you could change the scenario so that the loot is unusable and therefore worthless to them, why wouldn't you?

Behavioral authentication provides just such an opportunity. When what thieves need in order to commit cyber fraud can't be stolen, they're sunk. This method makes all that stolen data unusable, protecting not only customer data but your brand as well. Data breaches will become less likely as well, since there's no point trying to steal things that have no value in themselves. Consumers can feel confident about using your site, and you can rest easier at night.

About the Author:

Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management and protection of complex information systems – leveraging people, process and technology to counter cyber risks. Robert can be reached on Twitter and through the NuData Security website.

CYBERTECH
29.9.2016 // EUROPE

in collaboration with LEONARDO

FOR CYBER DEFENSE MAGAZINE READERS!
10% OFF
cdm 92783484

CYBERTECH EUROPE

CYBER // INNOVATION // ADVANCED TECHNOLOGIES // INVESTMENT OPPORTUNITIES

29.9.2016 Join us at Palazzo Dei Congressi In Rome, Italy

Cybertech Europe is the premiere event focused on technology, cyber and investment

Also featured is the 'Cybertech Innovation Pavilion' featuring the most innovative startups from around the world

Don't miss this unique networking opportunity!

ORGANIZED BY:
CYBERTECH

E: info@cybertechitaly.com // W: italy.cybertechconference.com

Five Recommendations to Enterprises in the Middle East for Improving Network Security

Cherif Sleiman, General Manager, Middle East and Africa at Infoblox

In May this year, we posted results of our 'network protection survey', which looked – among other things – at best practices in companies that were highly successful at network security. I will drill down into these best practices, and how to achieve them.

Some of the recommended actions have the added benefit of positively influencing multiple outcomes, so organizations in the Middle East can benefit by prioritizing these actions first.

Recommendation #1: Get rid of departmental silos.
Among survey respondents, there was a high correlation between those who reported best results with those who enjoyed a high level of cooperation between network, security, and application teams. You may need to retain data silos to ensure privacy and security, but colleagues should be made aware of those limitations.

Technology can be a great facilitator to enforce essential policy and remove artificial boundaries or silos that limit data sharing across groups.

Recommendation #2: Pay attention to operational realities.
In network security and network operations (and probably most areas of the enterprise), technology alone will not alleviate certain realities about doing business. Technology must be part of a strategy to optimize processes and help people make intelligent, intuitive decisions based on information (not data) and enriched with the right context.

Recommendation #3: Prioritize based on risk analysis.
Actions should balance risk and reward. That requires laying the foundation for intuitive decisions with information and context derived not from all data, but from data required to provide a perspective on risk and impact on the business.

Human beings should not have to correlate data themselves or use guess work to determine impact.

To prioritize properly, they must have as much aggregated context as possible (that's why getting rid of silos is so important).

Recommendation #4: Be realistic about security staffing.
Finding staffers who are experienced in three key areas – networks, security, and applications – is no picnic.

Sometimes finding an expert in just one area is difficult. If you do find them, they're likely to be expensive and in demand.

That's why it's important to look for technology that reduces the need for adding staff with cross-departmental expertise and can augment existing staff with insight that would have required additional manual work or resources.

Recommendation #5: Automate routine tasks.
Automation has value beyond avoiding mundane tasks and freeing people to make better decisions. It helps reduce delays and errors, as well as identifying incorrect or inefficient processes, while avoiding ad hoc workarounds.

As survey respondents reported, automation institutionalizes tribal knowledge and allows staff to react more consistently when faced with certain situations.

Perhaps our key recommendation from the network survey is to remember that every solution encompasses people, process, and technology. Overreliance on any one is hardly ever the right answer or approach.

About the Author

Mr. Sleiman has more than 20 years of sales, technical and business experience with some of the world's leading networking and telecommunications technology companies.

He has held key executive roles, including chief operating officer and chief technology officer at Core Communications, a software and IT services company focused on cloud-based business services and web and mobile apps.

He spent more than six years at Cisco in various leadership positions, the last being senior director, leading the enterprise business for Middle East and Africa. He also developed the strategic vision and technology roadmap, and managed all aspects of research and development, for Nortel Networks in his role as CTO, Enterprise Business Unit.

Why The Human Element Is The Biggest Point Of Failure In Your Data Center

You've probably taken pretty extensive measures to protect the servers in your data center. But have you covered everything? What about your employees?

by Tim Mullahy, General Manager, Liberty Center One

Here's a story for you: you're managing a high-end data center.

Your servers are properly maintained, and your server room is fully climate controlled. You've multiple backup generators, and your network routes are fully redundant. On paper, your facility is functionally immune to downtime.

Then you wake up early one morning to a notification, and hear words that send a chill down your spine. Catastrophic failure. Unscheduled downtime. Lost data.

What happened?

Turns out that in spite of all the measures you took to keep things running, somebody failed to follow your maintenance procedure. Hardware that should have been examined and replaced was left running, and that eventually cascaded into something far, far worse than a few bum components.

Disasters and unavoidable failures can happen, but the core truth of data center management is that 70% of outages can be directly attributed to human error.

Just look at the recent downtime at Spark, New Zealand's largest telecom provider. Although inclement weather did play a role in downtime, had Spark been examining its infrastructure for ongoing weaknesses - the downtime would have likely been much reduced.

If you'd like another example, look at what happened with Swedish infrastructure company Telia, a network provider which had an engineer inadvertently send all of Europe's traffic to Hong Kong.

It isn't just human error, either. Disgruntled employees can cause just as much harm to your data center as ignorant or careless ones. Incidents such as the 2011 equipment theft at Vodafone or the 2015 storage device theft at RSA can cause an outage, a PR disaster (complete with legal and regulatory fines), or both.

In short, it's in your best interest to reduce the risk that someone's going to mess something up - either intentionally or otherwise.

Cutting Down On Employee Risk

There are a number of things you can do to reduce the chance that an employee will bring your entire facility crashing down around your ears. Establishment of proper procedures for maintenance, monitoring, and documentation is the first step. But there are also a few additional measures you should take:

1. Have an emergency preparedness and response plan in place should an outage occur. Who needs to know about it? Who's responsible for addressing it? How should it be reported?

2. Regularly evaluate your hiring process to ensure that you're only bringing in the most competent and skillful professionals and engineers.

3. Institute a mandatory, regularly refreshed training program that details workplace safety, data center procedures, roles/duties, security information, etc. As an aside, make sure roles and duties are clearly defined for each employee.

4. Ensure you've always the necessary professionals on-shift - technicians with electrical and mechanical expertise are especially valuable.

5. Control access to restricted areas - An electrician might need to be in the server room to check equipment, but does an IT administrator really need access to the room in which your switches are stored?

About The Author

Tim Mullahy is the General Manager at Liberty Center One. Liberty Center One is a new breed of data center located in Royal Oak, MI. Liberty can host any customer solution regardless of space, power, or networking/bandwidth requirements. Tim can be reached on Twitter at @LibertyCenter1 and at his company website, Liberty Center One

CYBERTECH

6-7.9.2016 // SINGAPORE

YourSingapore

FOR CYBER DEFENSE MAGAZINE READERS!
10% OFF
cdm 92783484

CYBERTECH SINGAPORE

CYBER | INNOVATION | ADVANCED TECHNOLOGIES | INVESTMENT OPPORTUNITIES

6-7.9.2016 // MARINA BAY SANDS, SINGAPORE

FIRST EVER IN ASIA!

START-UP PAVILION FOR CYBER COMPANIES

AMONG THE SPEAKERS

BG. (Res.) Dr. Dani Gold
Head of MAFAT, Israeli MoD

Mock Pak Lum
Chief Technology Officer
StarHub

Mr Teo Chin Hock
Deputy Chief Executive,
Cyber Security Agency of
Singapore, CSA

Prof Lam Khin Yong
Chief of Staff & VP
(Research) at Nanyang
Technological University

Victor Yeo
Deputy GM, ST Electronics
(Info-Security) Pte Ltd

INDUSTRY PARTNER StarHub | ACADEMIC PARTNER NANYANG TECHNOLOGICAL UNIVERSITY

STARHUB ECO SYSTEM: FORTINET BLUE COAT

Check Point SOFTWARE TECHNOLOGIES LTD | CYBERARK | CYBERBIT PROTECTING A NEW DIMENSION | IAI | RAFAEL ADVANCED DEFENSE SYSTEMS LTD. | ADALLOM | Microsoft | COBWEBS TECHNOLOGIES

Mellanox TECHNOLOGIES | Custodio | Israel Electric | THETARAY | DARKTRACE | JVP | SANS | vertex | FIRMITAS Cyber Solutions | IMI SYSTEMS

E: cyber@cybertechsingapore.com // W: singapore.cybertechconference.com // P: +65-6809-2205 // F: +65-6809-2001

The Rise and Warfare of Ransomware

What is Ransomware?

Ransomware is compiled of two words which is Ransom and Ware. As you could guess Ransom sounds like a hostage situation you see in the movies where someone is held in exchange for a large amount of money. Ware is from the term Malware (It is a term used for intrusive or disruptive software.)

Ransomware can therefore be compared to the common ransom methodology approach, where a person is held captive and only released in exchange for a sum of currency. However in the IT world this is commonly your files.

How does it work?

First an attacker would go about infecting your system with ransomware. This could be done via social engineering, breaking into your system, or by a user plugging in an already infected device. Once the ransomware gets into your system, it will then work its way through your system using cryptography to encrypt as many files as it can find. Once this is completed, a ransom message is displayed instructing you to pay bitcoins to get access to your files again. Commonly there is a counter displayed on the screen ticking down before your files are deleted.

Using companies such as Western Union and Bitcoin, where you are able to send money to others without being easily traced. Therefore attackers leverage this system of not being easily caught. Most recent ransomware commonly provide a link directly to a bitcoin payment portal.

An easier way to understand how ransomware works is by the following points:

1. Infect and spread
2. Encrypt
3. Demand payment

In the “infect and spread” phase the system has already been compromised and the ransomware is using its malware ability to begin its assault on your system. In its arsenal is a program which is working its way through your network looking for other devices it could connect to and infect with its payload.

Next the “Encrypt” phase begins. The ransomware encrypts all the files that meet the prerequisites set by the attacker. The private key that can decrypt your files is sent back to the attacker and deleted from the infected system..

The final phase of this attack will be to demand payment. All the victim can see at this phase is that double clicking an encrypted file launches a window demanding sums of money for files to be unlocked or they will be automatically deleted within X amount of time.

Who does this effect?

I have seen and heard of many stories were databases have been hit by ransomware. This includes payroll systems, client databases, supplier databases or even whole business file servers that hold client confidential documents.

The big question that sits on most entrepreneurs and Chief executives tongue is “Will I go out of business?” I have personally seen ransomware asking for 500 USD per file to be unlocked.

Popular ransomware Cryptowall, cost the US alone 18 million pounds. This particular ransomware demanded 200 – 10,000 USD. Cryptolocker has been documented to have made 30 million USD within 100 days. Although these statics are written according to the US, You must note:

- The UK is still in the top 10 countries hit by ransomware.
- Around 48% of users in the UK hit by ransomware will pay the ransom
- The UK is one of the countries that get hit by higher ransoms.
- Just under 55% of all spam emails in the UK now have some form of ransomware/Malware attached within it.
- Ransomware attacks in the UK are growing as one of the most popular methods to attack organisations
- Businesses with over 10 employees are the most common targets

The above points make it clear that black hat hackers are interested in the easy and quick cash in option. Ransomware is now on the rise as the most popular and profitable method of attack.

Staying Safe

Most businesses do not have a strategic solution for recovery from an attack. Most attacks that lead to a system being comprised, have at least 2 days down time and lock at least 72% of employees out of their data for that period.

First we should cover the obvious points of preventing your system from being a target.

Configuring spam filters and email virus scanners will help reduce the chances of being infected by ransomware, as most ransomware is delivered through an infected email.

IT Security Policy & Privileges, users should be prevented from plugging in removable storage. This includes their mobile phones, USB drives and other devices, in case their device is infected with ransomware. Users should not be granted more privileges than needed on each system. Should ransomware use their account, then the damage would be limited to only files they have access to.

User Training is important to make employees aware of different types of attacks. Maybe even looking up and sharing a case study with employees would help them to better understand and evaluate the risk.

Data Backups should always be kept safe and offline, as you do not want to do be writing over you're backed up data with the ransomware data. In case you are already infected, consider a recovery strategy that best suits the situation.

Anti-Virus software is important but also make sure you are running the latest anti-virus and have the latest definitions applied. Further make sure your policies are configured correctly and new devices installed on the network are also placed in the correct group so they are managed correctly.

SILO. It is a good idea to cordon parts of your network off and install firewalls between each area. This includes packet inspection and Intrusion detection systems and intrusion prevention systems. Web filtering would also be recommended. This not only helps protects your vital systems from attacks but can also prevent ransomware from spreading. Segregating your network forms a barrier that filters legitimate and non-legitimate traffic to help prevent the ransomware from spreading across the network.

What to do if I am attacked

If you have a valid offline backup, you may think it's as easy as restoring the data. But this is not the case when it comes to ransomware. You do not want to risk your backup also getting infected. The most important step to take is to identify the ransomware. Then implement the necessary steps to remove it from your systems. After doing so you can simply restore the data. If you do not have a backup of the file(s) to restore, then your options are to either have someone take a look at reversing the key to unlock the file or pay the ransom. It's best to have a look at your IT system sooner rather than later to avoid a situation like this. Meta Defence Labs have a service where they provide a "no crack no fee" service. They will take a look at the file for you to reverse engineer or provide consultancy to help clear an infected environment. Their auditing services can also help provide a better idea on weak points in your network to harden your environment.

About the Author

Harpreet Bassi. I have worked in IT and Information security for the past 14 years. During this time I have experienced how companies cut corners with their IT budgets where security is not always checked and tested enough. Together with some colleagues, we formed Meta Defence Labs that offers affordable and reliable security and infrastructure solutions to our clients. At Meta Defence Labs we provide customised and affordable cybersecurity and secure infrastructure solutions to our clients.

- Website: www.MetaDefenceLabs.com
- Twitter: https://twitter.com/MetaDefenceLabs
- Facebook: https://www.facebook.com/MetaDefenceLabs/
- LinkedIn: https://www.linkedin.com/company/meta-defence-labs-ltd?trk=biz-companies-cym"

IN SUPPORT OF THE GOVERNMENT'S ICT SPEND OF USD $20 BILLION OVER THE NEXT 5 YEARS

EXPO COMM INDONESIA 2016™

BROADBAND – CYBER SECURITY – SMART CITY INFRASTRUCTURE

9-11 NOVEMBER 2016 | JAKARTA CONVENTION CENTER

DELIVERING SMART SECURE CITIES THAT ENABLE OUR DIGITAL ECONOMY

Hosted by

Ministry of Communications and Informatics

ASOSIASI PENYELENGGARA TELEKOMUNIKASI SELURUH INDONESIA
Association of Indonesian Telecommunication Providers

Supported by

KADIN INDONESIA
Indonesian Chamber of Commerce and Industry

Coordinating Ministry of Economic Affairs

WANTIKNAS Dewan Teknologi Informasi dan Komunikasi Nasional
National ICT Council

APEKSI
Association of Indonesia Municipalities

Sponsored by

Telkom Indonesia
the world in your hand

ARIM Technologies

Organized by

infrastructure asia

Tarsus

Co-Organized by

EJK E. J. Krause & Associates, Inc.

Media Partner

CDM Cyber Defense Magazine

WWW.CONNECTINDONESIA.NET

PART OF Indonesia Infrastructure Week

Runtime Application Self Protection

For its proponents Runtime Application Self Protection (RASP) represents not just the next generation of application security but a quantum leap forward in how Cyber Security can bring benefits to business beyond protecting assets and reputation.

Runtime Application Self Protection (RASP) is a term used to describe security technologies that are embedded within the application tier which can detect and prevent runtime security exploits.

Since its emergence in 2012 RASP, a term coined by a Research VP and Gartner Fellow Joseph Feiman, has witnessed an increase in adoption commensurate with greater awareness of the benefits of RASP.

What Distinguished RASP from WAF?

Unlike Web Application Firewalls (WAF) that occupy the perimeter space of IT security and which attempt to protect applications by analysing Web traffic in order to identify malicious activity using known attack signatures, RASP based technologies leverage their access to runtime application data to prevent vulnerability exploitation.

This approach promises to eliminate false positives and significantly reduce the complexity and management effort of mitigating the most common vulnerabilities being exploited today.

By embedding security intelligence directly within the application tier RASP technologies can differentiate between application and user data allowing them to identify maliciously injected code (tainted code) or to detect unusual application activity (indicators of intrusion) with an unprecedented degree of precision. When compared to the high rates of false positives produced by WAF and indeed incidents resulting in service disruption due to poorly configured firewall rules, the contrast is stark.

RASP security rules can be configured to raise alerts or prevent attempts to access protected compute resources such as file systems and network sockets.

Depending on the capabilities of the specific implementation of RASP these rules can be simple, generic and dynamically adjustable at runtime without impacting the normal application lifecycle or expected application operations.

Some of the most exploited vulnerabilities (as classified by OWASP) that RASP technologies protect against include SQL Injection, Command Line Injection and Cross Site Scripting. Mitigating SQL Injection using WAF typically demands the creation of multiple rules that attempt to match as many permutations of SQL injection input data as possible while trying to avoid matching genuine requests.

The problem is compounded by having to create and maintain nearly identical rules for different URLs in the worst case scenarios. These drawbacks also apply to Cross Site Scripting and Command Line Injection and other attacks.

When we compare the WAF approach to the more mature RASP implementations which can disable all SQL Injection with almost 0% chance of generating a false positive with a single one-line rule, the benefits of RASP to the business start to become clearer. The same can be said for mitigating other vulnerabilities and while some instances may require slightly more work than defining a single rule, the configurations are far simpler and more robust than their WAF analogues.

The simplicity and power of RASP in the sphere of vulnerability mitigation alone makes a strong case for including RASP technology as part of a comprehensive Cyber Security strategy. This is especially true for Java applications. Java's ubiquity in the enterprise and the frequency of new vulnerabilities being identified in open and propriety APIs as well as the 90-day Critical Patch Update (CPU) cadence of the Java Virtual Machine (JVM) itself all contribute to the difficulty and cost of securing Java.

However, recently two other significant benefits of RASP have come to the fore namely Zero Day Vulnerability mitigation and Virtual Patching.

Blocking Common Zero Day Attack Vectors

The generic nature of the rules that can be configured for RASP technologies means that they can disable the most common execution vectors exploited by Zero Day Attacks.

For example, a RASP enabled Java Virtual Machine can be configured to deny the creation of client and server sockets or file descriptors, either entirely if the application has no need of them or allowing descriptor creation for the exact port numbers and file locations used by the application.

This fine grained control can stretch to every aspect of the runtime so, in keeping with our Java example, RASP could prohibit access to specific classes or packages irrespective of the any other native Java security facilities. While the vulnerability still exists in the application logic, exploits are rendered harmless and alerts can be raised for further investigation when illicit attempts are made to access protected resources.

While this kind of fine grained resource access control can be configured at the OS or Hypervisor level it remains cumbersome and error prone for many large enterprises to manage application security at the OS level. The cost of having an infrastructure team attempt to manage the security of large numbers of applications using OS level resource control gets more and more expensive and time consuming with each new application.

Another drawback of OS level resource access control is that affecting a change to an application's security profile will normally require the application to be restarted. While this may not be an issue for low SLA applications in small numbers, for large enterprises with thousands

of applications, operating under critical SLAs, the operational impact will be significant both financially and temporally.

Virtual Patching

Virtual Patching is the ability to host legacy code within a virtual container that effectively secures the application as if it was running in an updated and compliant version of the runtime. This is important for enterprises with mission critical legacy applications that cannot be upgraded due to technical constraints or lack of expertise.

Every established large IT consuming enterprise has these legacy applications and while there is always a plan to replace these systems with entirely new applications over time, until they are replaced they pose a significant risk to the business, risks that may violate the demands of regulators. More often than not enterprises hit a brick wall where they simply have to acknowledge that they cannot replace certain components and must resort to mitigating the risks posed by legacy systems.

RASP implementations with Virtual Patching capability gives the business the option of safely containing legacy applications, running them on up to date and compliant runtime environments but without requiring the recompilation or the code changes that would be demanded by a physical upgrade or having to rush transformation projects to avoid legal and commercial risk.

Virtual Patching can also refer to the ability to replicate the effect of binary patches with RASP. For example, RASP can be used to replicate CPUs issued by Oracle for Java on a quarterly basis giving businesses the option of obviating the need to apply CPU binary patches. This is important for the enterprise as applying binary patches to hundreds or thousands of JVMs can be complicated process requiring not only engineering resources put also scheduled down time to affect the patch and allow application teams to complete their testing.

For large enterprises with complex patching processes that demand considerable orchestration between development teams and operations to organise, this aspect of Virtual Patching provides considerable cost saving and reduced risk when compared to binary updates. Depending on the implementation of RASP, Virtual Patching can be a non-intrusive, centrally manged, operation that can dynamically patch applications without disruption to normal operation or scheduled down time.

Choosing the Right RASP Implementation

There is considerable variety in the way different vendors implement RASP. Enterprise users need to consider the impact of integrating and deploying RASP technologies in their IT estates. Careful consideration needs to be given to the impact of any code or configuration changes that may be required to enable RASP on the applications that run on their platforms.

Many RASP vendors claim that no code changes are required or that configuration and performance impact are minimal. However, what may seem to be a trivial code or configuration change, when scaled to hundreds or thousands of applications can considerably impact the speed of adoption of RASP.

A well informed, scoped and executed proof of concept is absolutely essential in the vendor selection process, but just as importantly for enterprise customers is a proven track record in production and customer references. The claims of some RASP vendors demand careful scrutiny.

A common critique of RASP is the expected performance impact of runtime analysis and protection. Early implementations of RASP could cause as much as 10% increase in response times within the application tier and so were generally deployed to applications with SLAs that could accommodate such degradation.

Performance is constantly improving with many vendors now claiming 5% or less impact on application response times. In general, other bottlenecks in the technology stack make far more significant contributions to performance loss and response times for example, database access or internet latency.

It should also be remembered that rewriting insecure code to carry out the kind of protection delivered by RASP will in most instances cause a similar impact to performance.

The Current State of Play

In 2014 and 2015 a number of RASP vendors announced commercial engagements that set the stage for RASP to be fully tested in enterprise production environments. In most instances we find the majority of those RASP vendors and their deployments have met the expectations of their customers and piqued the interest of their competitors.

These early adopters are now driving the direction of RASP technologies and reaping the benefits RASP. We can expect the rate of adoption of RASP to continue to increase in 2016 especially in heavily regulated sectors that are seeking innovation to meet the demands of global, regional and state regulators in the most cost efficient manner.

Key sectors where we can expect RASP to flourish fist include the Financial sector, Health and Defence.

About the Author

Hussein Badakhchani is a Distinguished Technologist with over 20 years of experience in IT spanning software development, system integration, IT architecture and design, DevOps, IT strategy and innovation.

As a thought leader and trusted advisor, Hussein provides critical analysis of technology and its use to executive IT decision makers in Government, Banking and Financial sectors.

Why Don't More Sites Use HSTS To Protect Their Users?

HSTS is a security mechanism that helps prevent a potential circumvention of SSL encryption, ensuring that sensitive data isn't exposed.

SSL has generated an unusual amount of attention recently, and mainly for reasons detrimental to the trust that users need to have before sending private data like credit card numbers over the Internet. Heartbleed aside,

SSL is a relatively securely protocol for encrypting sensitive data: it's mathematically sound and, aside from implementation errors, makes is practically impossible for malicious third parties to intercept data moving between a browser and server.

SSL is great as far as it goes, but it isn't yet integrated well enough into client applications like browsers to be entirely relied upon.

Consider this scenario. You're sitting in your favorite coffee shop, browsing pictures of pastries on Pinterest, and you decide to take a look at your bank balance before investing in a chocolate muffin.

You connect to your bank's website and note that an SSL session has been initiated. You then login, check your balance, and, satisfied with your financial health, head off to buy your muffin.

When you noticed that your browser had initiated a secure SSL encrypted connection, there would ideally only be one possible explanation: your browser had initiated a secure SSL connection.

But, unfortunately, there is another explanation: someone intercepted your WiFi connection and interposed themselves between you and your bank.

They received everything your bank sent to you, changed it in any way they pleased, including altering the code so that the favicon looked like a padlock, and they now know exactly how desperate you were for a chocolate muffin.

But, I hear you thinking, if the connection wasn't secure my browser would have told me — it's always popping up warnings about this or that site being insecure. Well, yes and no. If your browser finds something wrong with a secure connection, it will tell you.

But it won't tell you if a connection you believe to be secure isn't, because it doesn't know that it was supposed to be secure in the first place.

That's the problem HSTS is supposed to combat. The HTTP Strict Transport Security mechanism allows a web server to declare that it will only interact using an SSL / TLS

connection.

The server will send an HTTP response header to the browser that specifies a time-frame in which the browser must connect only using a secure connection.

In our coffee shop scenario, the hacker intercepted the bank's web page data and made it appear to be secure to a casual human observer.

The browser didn't care that there was no SSL connection in reality, because it had no reason to expect that there should be one. HSTS allows a site to say upfront: "I should be encrypted," which allows the browser to reject unencrypted connections that appear to originate from that site.

Of course, there is a weakness in this system too. If the attacker can intercept the very first stages of the connection, he can modify the HTTP header that is supposed to tell the browser to accept only SSL connections. Firefox and Google Chrome mitigate this risk somewhat by including pre-loaded lists of HSTS sites, but that's not scalable.

Nevertheless, HSTS improves security on the web and helps avoid SSL-stripping attacks like the one described above.

Because it's easy to implement in popular web servers, and is supported by most browsers, the question arises: why do so few website use HSTS.

About the Author

Matthew Davis -- Matthew works as an inbound marketer and blogger for **Future Hosting**, a leading provider of VPS hosting.

Follow Future Hosting on **Twitter** at @fhsales, Like them on **Facebook** and check out their tech/hosting blog,**https://www.futurehosting.com/blog/**.

Latin CIO Summit

November 17-18, 2016, Trump Ocean Club, Panama City, Panama

Industry leaders from around the globe are confirming their places on the line-up for the Latin Chief Information Officer Summit. Join them in a two day event offering Latin America's leading decision makers of the industry a devoted environment for **unparalleled business and networking opportunities in a stimulating environment.**

Grow your business & sales in just 2 days
Network with high level executives during formal and informal time such as cocktails and dinner hours!
Target qualified buyers through our pre-scheduled one-on-one meetings format

EXPERT SPEAKERS ALREADY CONFIRMED ON THE LINE-UP INCLUDE

- EVP & Chief Information Officer, **Costco Wholesale Corporation**
- Chief Information Officer, **Xerox Corporation**
- Global Product Security & Services Officer, **Philips Healthcare**
- Chief Information Officer, **Georgia-Pacific LLC**
- VP, Global Technology Services, **U.S. Bank**
- Senior Vice President, Head of North America, **Syntel, Inc.**
- Chief Technology Officer – Americas, **HCL Technologies**

SOME TOPICS TO BE DISCUSSED ARE:

- The Role of the CIO
- Data Security
- Mobility and Network Connectivity
- Trends and Uses of The Cloud
- Big Data
- IT Working Together with Sales and Marketing
- Adapting to the Fast Forward Digital World
- Investing in Talent
- The future of Technology in Latin America

For more information please contact **alejandrad@marcusevansmx.com** or visit
http://events.marcusevans-events.com/latinciocdm

marcusevans

How to protect your critical asset from the insider's threat?

By Milica Djekic

The modern times bring us lots of concerns regarding terrorist attacks and diversions. The goal of terrorism is to produce a fear and make victimization of the targeted groups. The common target of terrorist attacks is a critical infrastructure which is part of the country's assets which is vitally important to its nation.

The consequences of the critical infrastructure damage or loss could get catastrophical to such a society. Through this article, we will discuss why it's so dangerous to suffer the critical asset's diversion as well as deal with someone who would support the entire action from the inside.

The critical infrastructure requires people to work for it and maintain its capacities. That infrastructure could include any strategically important facility to the country including water supply systems, telecommunication facilities, airports, water waste systems, power plants and so on.

It is clear how risky it would be if someone from inside shared confidential information with the threat from outside or allow an access to that asset to such a malicious actor.

If we try to imagine the consequences of such a prepared attack – we would realize that they could get catastrophical to that organization, its employees and the entire nation.

For such a reason, it's so important to put every critical asset under the exposure and constant monitoring by defense professionals. Some risks could be prevented and some insider's threats could get recognized before they harm their surroundings.

We are aware that not everyone can be employmed within some critical infrastructure and so commonly those people are trusted in a security sense. On the other hand, many developing countries would face the internal diversions for many reasons.

For example if the employer paid the staff member well they wouldn't turn to terrorism. Also, every attack to a critical infrastructure may get considered as an act of terror.

Everyone involved in such an operation would get a status of terroristic fugitives.

Unfortunately, not even the developed societies are immune to those threats because their community is so diverse in background. Many westerns would join the terrorist groups and work for them silently taking out many confidential findings and participating into diversions, sabotages, espionages or any other sorts of attacks.

A good way to assure your critical asset or any other organization is to manage your staff members smartly and securely.

Attempt to identify the potential threats through routine controls, assessments or interviews. In other words, some safety, security procedures and policies must get followed and the employees should be aware of the importance of their responsibility to the entire nation.

In addition, working as insider's threats – they could put their own safety and security under risk, so they should think twice before they accept any offer from the outside.

Also, it's recommended that those staffs should periodically report about their external contacts, travelling aboard or any other private businesses being correlated with the interests of that organization.

Finally, we would suggest that the critical asset's organizations should take full care about their employees and safety and security of the entire nation and country.

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.

Can Your Company Protect Itself From Ransomware?

Ransomware attacks are a frightening prospect for any business, but education and backups can take the sting out of ramsonware's tail

Consider the position your company would be in if it suddenly lost access to its data. Every email, customer record, document, and business plan — all gone in the blink of an eye. Many businesses would be out of business if that happened. Revenue streams will dry up.

Staff will sit twiddling their thumbs or be sent home. This scenario is a nightmare for any business owner, and it's exactly what happens during a ransomware attack.

Ransomware is a brutal type of cyberattack in which a company's files are encrypted. The attackers demand payment in exchange for the key that will decrypt the data.

Once your files are encrypted, there is nothing you can do to get them back short of paying the ransom. You may have heard stories of successful data recovery by security experts, but it's a mistake to bet on that. Ransomware has become increasingly sophisticated and the flaws that were present in early versions have been removed.

The encryption technology used is extremely powerful — the sort of stuff the NSA can't crack.

However, there are ways to protect your company by both reducing the chances of a successful ransomware attack and being prepared in case your data is encrypted.

Educate Your Employees

In order to carry out a ransomware attack, the attacker needs to get malware into the company's network. The attacker might exploit weaknesses in the network to gain access, but the majority of ransomware attacks start with either a phishing email or a malware site visited by an employee.

Employees are the front-line of any company's security. That doesn't include only system administrators, IT professionals, and network engineers.

It includes everyone, because any employee can click on a link in a phishing email or accidentally visit a malware-laden site.

Companies should make sure that all employees with access to computers inside the company network understand the risks of clicking links in suspicious emails and that every email should be viewed with suspicion.

Employee education is the first line of defense against ransomware.

Backup

Online criminals are smart, and many employees lack the technical proficiency to understand the scope of security risks posed by phishing emails and other sources of vulnerability.

Education is essential, but it's best to assume that a ransomware attack will be successful at some point, and prepare accordingly.

Ransomware attacks only work because the attacker can use the threat of permanent data loss. Comprehensive, up-to-date, offsite backups remove the risk of data loss.

With a decent backup in place, recovering from ransomware attacks can be as simple as wiping the affected systems and restoring data from the backup.

There will almost certainly be some downtime, but it's better than paying the ransom.

Without comprehensive backups, a company may have no other choice than to pay the attacker.

Ransomware attacks are a frightening prospect for any company, but it's not difficult to mitigate the risk of data loss. A catastrophe that puts your company at grave risk or a minor inconvenience? Preparation can make all the difference.

About the Author

Justin Blanchard has been responsible for leading initiatives that increase brand visibility, sales growth and B2B community engagement.

He has been at the core of developing systems, tools and processes that specifically align with Server Mania's client's needs.

Finding real-world solutions to complex business security problems

News cycles are dominated by ongoing reports of cybersecurity issues and it is expected that by 2019, the cost of cybercrime could rise to over $2 trillion dollars.[i] In an effort to help businesses combat threats related to cybersecurity and increase protection protocols, a conference dedicated to offering real-world solutions to complex business security problems is taking place in Knoxville, Tennessee this October: EDGE2016 Security Conference.

Created as a response to the growing threat to businesses in a variety of industries, EDGE2016, presented by Sword & Shield Enterprise Security, Inc., will include speakers with cybersecurity expertise in the fields of banking and finance, healthcare, government, legal, manufacturing and retail.

For businesses in these key sectors, the costs related to each cyber-attack on their infrastructure continues to rise every year. The average cost of a data breach in the U.S. has grown from $5.40 million in 2013 to $6.53 million in 2015, [ii] with the anticipation that these numbers will continue to increase.

In addition to the costs associated with these reported attacks, research suggests that the actual costs on a per-business and global scale may be far greater than the numbers show, due to reluctance to report security breaches associated with data and industrial espionage for certain business entities.[iii]

Specific attention on mitigating cybersecurity risks is at the forefront of many of the world's leading organizations. Ginni Rometty, Chairman, President and CEO of IBM Corp., related these issues when speaking to the IBM Security Summit, stating "We believe that data is the phenomenon of our time.

It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."[iv]

EDGE2016 is offering the opportunity for business and government representatives with the authority to institute change within their organizations to learn the latest methodologies and tactics to deal with these ongoing threats.

In addition to training sessions and roundtables, EDGE2016 will also have industry-specific track sessions to benefit individuals who are interested in how to prevent and contain security issues within their specific industry.

EDGE2016 will also feature two well-known cybersecurity experts as keynote speakers:

Theresa Payton

The first female to serve as White House CIO, Theresa Payton oversaw IT operations for the President and his staff from 2006 to 2008. Previously holding executive roles in banking technology at Bank of America and Wells Fargo, Theresa Payton has authored two books focused on assistance for protecting online privacy. She has been named as one of the top 25 Most Influential People in Security by Security Magazine and is considered one of the country's most respected authorities on internet security, data breaches, fraud mitigation and technology implementation.[v]

Kevin Poulsen

A former black-hat computer hacker who was convicted and imprisoned for cybercrime, Kevin Poulsen transitioned to become a white-hat champion of digital security and Webby Award winning journalist and writer in the area of cybersecurity and the law. A senior editor at Wired Magazine, Kevin Poulsen was the mind behind the influential "Threat Level" blog and has authored a book entitled *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* about imprisoned hacker Max Butler.[vi]

For more information on the EGDE2016 Security Conference taking place October 18-19 or to register for the event, visit https://edgesecurityconference.com/.

CELEBRATING 25 YEARS OF SUCCESS

25TH ANNIVERSARY

"Digital India"

Convergence India 2017

International Exhibition & Conference

8 9 10 February 2017 | Pragati Maidan, New Delhi

South Asia's largest ICT expo

Show Highlights

500 Exhibitors | 30 Countries | 150 Speakers from World over | 20,000 Visitors

Technology Showcase

• Telecom • Broadband • Internet of Things • Cloud & Big Data • Digital Homes
• Mobile Devices • Broadcast • Cable & Satellite TV • Film & Radio
• Content Creation, Management & Delivery

Co-located events and Add-ons

• Co-located IoT India 2017 expo • 4th Telecom Summit • GSMA Open Day
• Convergence India Excellence Awards • 2nd SCTE India Awards
• Start-ups Showcase • Mobile Devices & Accessories Zone
• Apps & Wearables • Smart Homes

Support
Department of Electronics & Information Technology
Ministry of Communications & Information Technology
सत्यमेव जयते Government of India

Media Partner
CDM CYBER DEFENSE MAGAZINE

Organiser
30 YEARS
Exhibitions India Group

For Exhibition & Conference, please contact:
Mr. Yash Menghani, Senior Manager, yashm@eigroup.in
217-B, Okhla Industrial Estate, Phase III, New Delhi 110 020
Tel: +91 11 4279 5000 | Fax: +91 11 4279 5098
www.convergenceindia.org

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

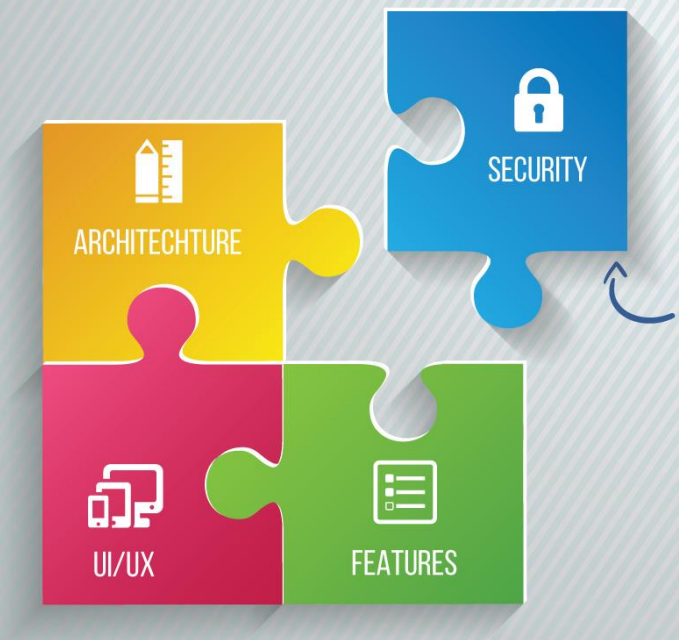
Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY



You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

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

VS.

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

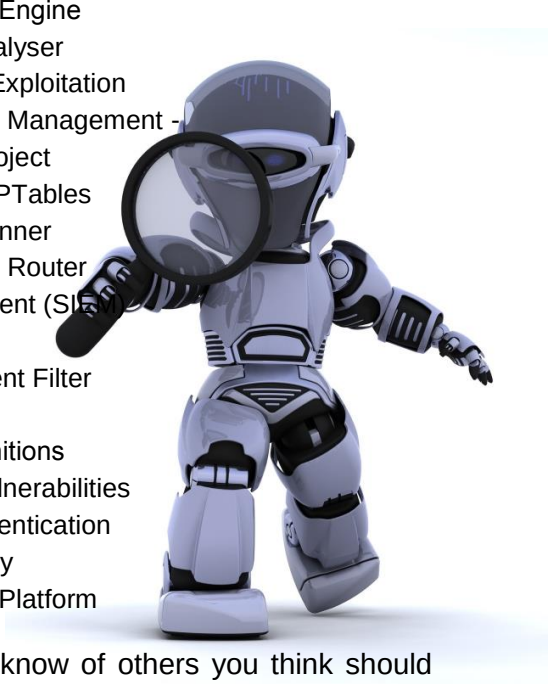
Top Twenty INFOSEC Open Sources

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

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

Here they are:

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



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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

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

So use it by going here:

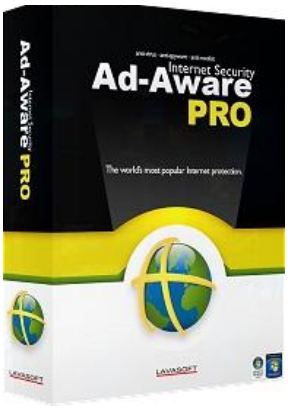
http://www.naisg.org/techtips.asp

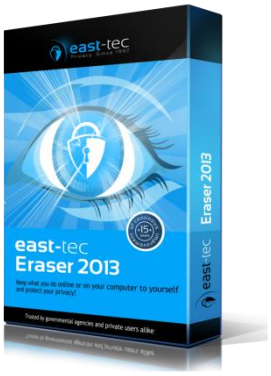
SOURCES: CDM and NAISG.ORG

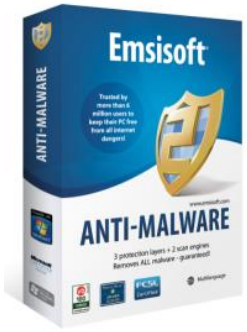
SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com

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







Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine August 2016

Sample Sponsors:

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

Cyber Warnings Newsflash for August 2016

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

Malware alert: Dump on WikiLeaks contained over 3,000 malicious files

http://www.computerworld.com/article/3110486/security/malware-alert-dump-on-wikileaks-contained-over-3-000-malicious-files.html

HANCITOR DOWNLOADER SHIFTS ATTACK STRATEGY

https://threatpost.com/hancitor-downloader-shifts-attack-strategy/120040/

Dridex Malware Targets Businesses

https://securityintelligence.com/news/dridex-malware-targets-businesses/

Eddie Bauer data breach: What you need to know about malware intrusion

http://www.al.com/business/index.ssf/2016/08/eddie_bauer_data_breach.html

Why Are The Congressional Intelligence Committees So Quiet On The NSA Malware Leaks?

https://www.techdirt.com/articles/20160822/01173235300/why-are-congressional-intelligence-committees-so-quiet-nsa-malware-leaks.shtml

Kaspersky Says that Shadow Brokers Leaked Malware is Genuine

http://www.spamfighter.com/News-20442-Kaspersky-Says-that-Shadow-Brokers-Leaked-Malware-is-Genuine.htm

NSA-linked hackers hoard malware secrets. What could possibly go wrong?

http://www.latimes.com/opinion/editorials/la-ed-equation-group-hacked-nsa-20160821-snap-story.html

Malware Targets Hillary-Haters With False Promise of Video Showing ISIS Payoff

http://www.forbes.com/sites/kevinmurnane/2016/08/23/malware-targets-hillary-haters-with-false-promise-of-video-showing-isis-payoff/#3aee4b1f23d7

Traditional malware falls, mobile malware on the rise

http://www.itproportal.com/2016/08/22/traditional-malware-falls-mobile-malware-on-the-rise/

PCVARK malware strain surfaces for the Mac, opens door for additional malware to be installed

http://www.powerpage.org/pcvark-malware-strain-surfaces-for-the-mac-opens-door-for-additional-malware-to-be-installed/

ATM malware costs Government Savings Bank $350,000

https://ibsintelligence.com/ibs-journal/ibs-news/atm-malware-costs-thailands-government-savings-bank-350000/

DroidOL: Android malware detection based on online machine learning

http://www.techrepublic.com/article/droidol-android-malware-detection-based-on-online-machine-learning/

Rex Linux Trojan, A New Multipackage Malware Spotted – Ransomware And Bitcoin Miner

http://techfrag.com/2016/08/23/rex-linux-trojan-malware/

Hackers Use Google's Ad Network To Spread "Fake Login" Malware

http://www.fastcompany.com/3062867/overlay-malware-google-adsense

Malwarebytes reports new OS X malware that could easily fool less technical users

https://9to5mac.com/2016/08/19/os-x-malware-mac-file-opener/

Now data-stealing Marcher Android malware is posing as security update

http://www.zdnet.com/article/now-data-stealing-marcher-android-malware-is-tricking-victims-by-posing-as-security-update/

'Project Sauron' malware hidden for five years

http://www.bbc.com/news/technology-37021957

Attacker's Playbook Top 5 Is High On Passwords, Low On Malware

http://www.darkreading.com/operations/attackers-playbook-top-5-is-high-on-passwords-low-on-malware/d/d-id/1326667

Credit Card Info exposed by POS Malware at some Starwood and HEI Hotels

http://www.bleepingcomputer.com/news/security/credit-card-info-exposed-by-pos-malware-at-some-starwood-and-hei-hotels/

New Banking Malware Touts Zeus-Like Capabilities

http://www.darkreading.com/vulnerabilities---threats/new-banking-malware-touts-zeus-like-capabilities/d/d-id/1326612

20 top US hotels hit by fresh malware attacks

http://www.zdnet.com/article/20-top-us-hotels-hit-by-fresh-malware-attacks/

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

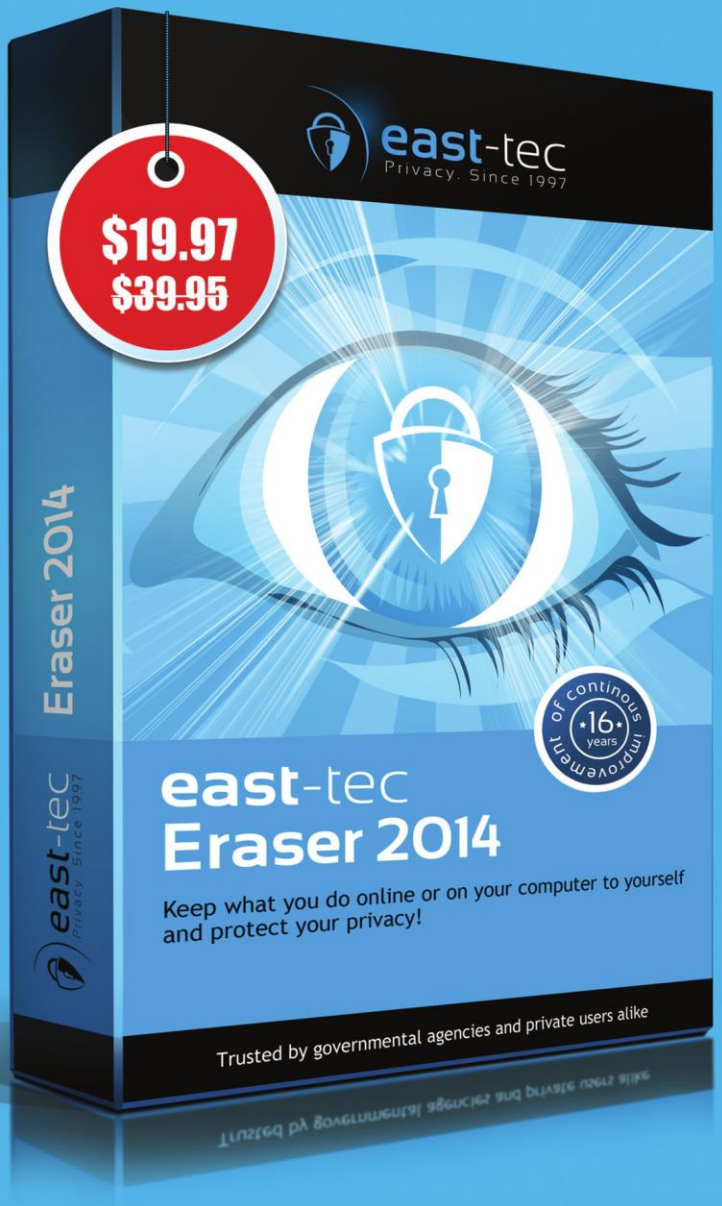
Cyber Defense Magazine - Cyber Warnings rev. date: 08/24/2016

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

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



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014