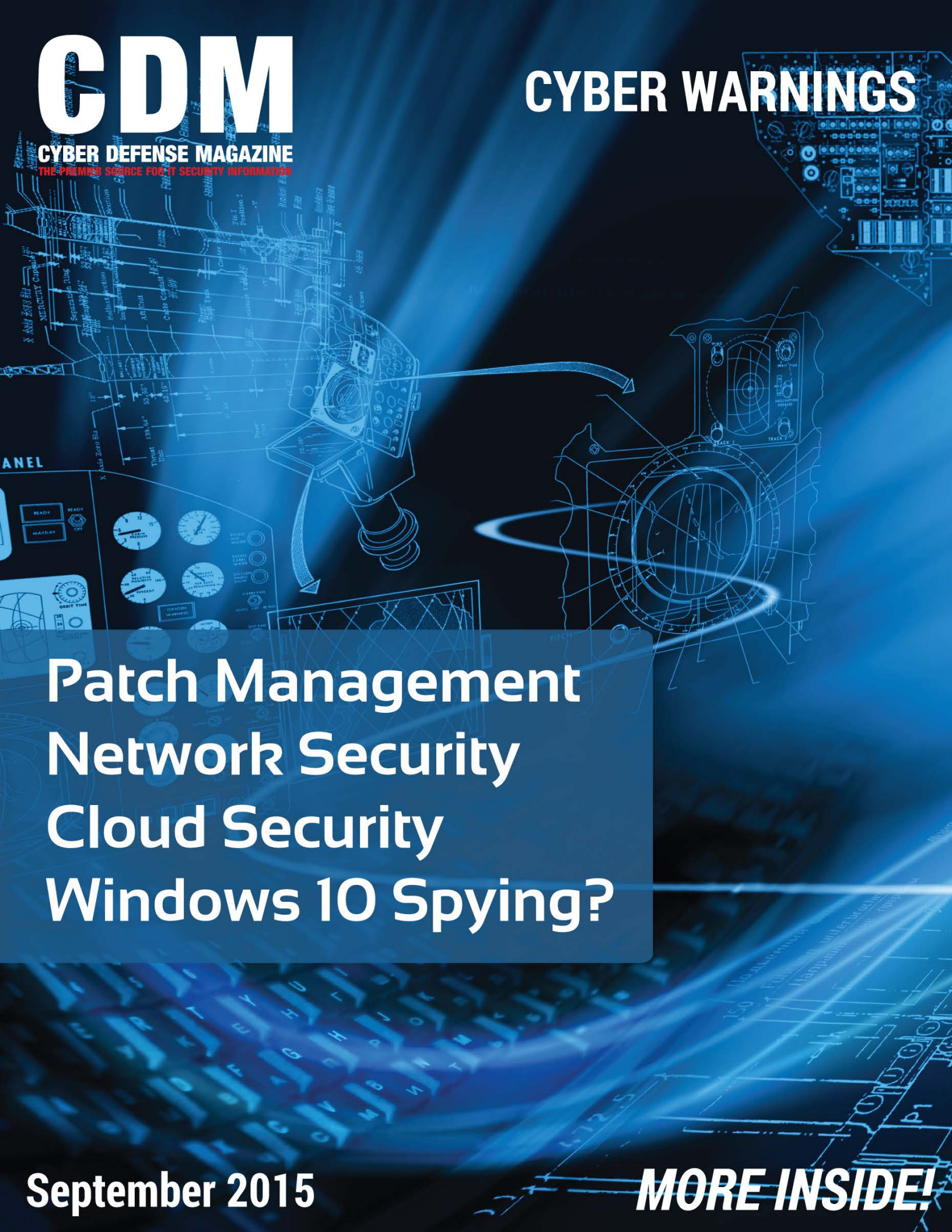


CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Patch Management
Network Security
Cloud Security
Windows 10 Spying?

September 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

Naren Vaideeswaran
Robert B. Dix, Jr.
Irena Mroz
Ofer Or
Scott M. Higgins
Moises Brito
Lenley Hensarling
Milica Djekic
Dave Wray
Lee Ying
Christian Mairoll
Anthony Scotney
Jean Lewis
Margie Sloan
Loucif Kharouni

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®

Managing Risk Requires Patience and Consistency

Friends,

In this month's edition of Cyber Warnings, we put a major focus on understanding Risk and dealing with key issues that help you reduce it. Not only is threat mitigation a key component, but also, patch management, consistently managed helps reduce your exposure.

There are so many new types of threats – whether it's they bring your own devices (BYOD) dilemma you now face or systems constantly being opened up to data leakage, mostly by accident of your employees. You also have to deal with the fact that new operating systems, such as Windows 10, aren't offered for free without a price – it's Microsoft, just like Apple and Google, gaining a foothold into your organization beyond what they should have, by deeply accessing private information and content – from images to voices and keystrokes.

We face a new challenge where the OS vendors themselves have accidently, for their own benefit, opened your network to backdoors for eavesdropping – whether by advertisement networks, malware or other cyber threats. So, it's truly a most important moment in time for network security to include privacy concerns in your risk management and mitigation strategy. Patching Windows 10, for example, may fix holes that reduce the risk of an exploitation by new malware, yet without turning off a plethora of privacy-risk features, native backdoors remain open and data leakage through your firewall could be happening without your knowledge.

I hope you will read through this edition of Cyber Warnings on the theme of risk management and mitigation by better understanding that patch management is incredibly important, but alone, it's only a tiny part of the new equation for network security. In addition, while the shifting of risk to the cloud, ie, other service providers might seem like a great approach, if you allow third parties to have any access to customer records or personally identifiable information (PII), your cloud services need to be as security and private and you would offer if you were managing the entire cloud offering, yourself.

To stay one step ahead of the next threat, you need to reduce risk at all network touchpoints and data access points under your control, even if you've offloaded the hosting to others. Ultimately, be consistent in your risk management analysis and be patient in your organization's adherence to your policies. With good training and a positive attitude, you can improve your security posture and mitigate the risk of exploitation.

To our faithful readers, Enjoy

Pierluigi Paganini

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

GEORGIA REGENTS UNIVERSITY'S SECOND ANNUAL

<Cyber Summit/>

<October 14-15/>

This two-day summit features senior military and government personnel leading cybersecurity and cyber education focused discussions.

There is no charge for Military, Government, GRU faculty/staff and students.

GRU GEORGIA REGENTS UNIVERSITY | CYBER INSTITUTE

To register: gru.edu/cybersummit/register.php

<J. Harold Harrison Education Commons Building • 1301 R.A. Dent Boulevard • Augusta, GA/>

10 Steps to a Better Patch Management Process

By Naren Vaideeswaran

Managing modern IT infrastructure in all its complex glory creates a tremendous amount of pressure. Add to this the ever-present threat of a cyberattack—not to mention a connected workforce that doesn't always consider organizational security a priority—and it becomes clear that preparedness is one of the most important things any IT professional can aspire to.

And a key element of IT preparedness, if not the key, is keeping systems and applications updated and fully patched. Although this might seem obvious, in the spirit of preparedness, ask yourself:

- How regularly am I performing security updates?
- How fast can I implement a software patch during a fire drill scenario?
- How effective is my overall patch process?

If answered honestly, it's likely that your response to at least one of those questions is not what it should be.

Thus, it's probably worth a reminder that patch management *is* the best strategy for maintaining security in your IT environment and *should* be a top priority for you.

That said, patch management is not without its challenges. After all, if it were, you would have been able to answer all the above questions perfectly. So, to help, consider the following 10 steps of an effective patch process.

1. **Keep an eye out for security vulnerabilities**
   There are several ways to check for security threats. It helps to have patch management software that notifies you of newly available patches.

   If you don't receive automatic notifications, you can manually check for threats via Internet searches or by signing up to receive security alerts and bulletins from US-CERT.

2. **Identify the impact of cyber threats on unpatched software**
   Not all security vulnerabilities and software patches will be relevant to your IT environment. Thus, it's good to categorize the impact of threats affecting security vulnerabilities using a scale of low, medium or high to help you carefully plan your next steps. Impact assessment is easier if you have comprehensive hardware and software inventory data.

3. **Prioritize patches**
   Unpatched software with critical flaws will compromise data, affect business productivity or both. However, rolling out all critical patches at once could break something in the network, and pinpointing root causes in such a situation is difficult.

   This is why prioritizing your patches is so important. Do this by assessing the risk of every critical vulnerability and the systems or groups that would be affected by a security breach.

4. **Create a backup plan**
   Design a contingency plan in case something does break during a patch process. You don't want to create a situation where you are patching several production servers at once without backing up critical data or making emergency repair disks.

   Back up the data on your workstations, too, and create a restore point or official image disk of critical files.

5. **Test patches first**
   Test your patches in a lab environment before rolling them out globally. This applies to third-party and custom applications.

   Identify and document the outcome of the patch operation, including tracking what breaks, where it breaks and how to fix it.

6. **Approve patches and define schedules**
   Approve software patches before rolling them out. If your patch management software supports update approvals, use this feature.

   This gives you better control over the patch process by making sure you approve only the patches that have been certified by the software vendor or tested in a lab environment.

7. **Patch frequently used computers first**
   Some malware targets your workstations and steals login information and personal data from your most vulnerable computers—the ones used most often for daily transactions. These are the computers that need to be patched first.

   If you can target users by Active Directory, that's an added advantage for targeted patch rollouts.

8. **Create pre- and post-installation scenarios**
   Cyber threats are most commonly aimed at Web browsers and Java and Adobe applications, so it becomes imperative to prevent failed updates by creating the right pre- and post-installation scenarios for successful installs, including starting or stopping services, terminating processes, etc. When testing the patch before deployment, make sure you decide on the right installation scenario, and replicate the same when deploying the updates.

9. **Assess the post-patch status**
   You might think you just patched over a thousand workstations and a few hundred servers, but your post-patch status report could tell you otherwise.

You must always assess your post-patch status by running a comprehensive report that tells you which computers did and did not install the updates, those that rebooted, failed to reboot, etc.

10. **Document and repeat**

    The complexity of the patch process differs depending on your organization's size and business requirements, but simplifying it is always a good idea.

    To do so, document the entire process following every successful patch deployment, which will simplify and streamline subsequent patches.

Following these steps to establish or streamline an effective patch management process can help you ensure you're able to answer with confidence the next time you are asked how regularly you're performing security updates, how quickly you can react to an emergency patch and how effective your overall process is.

Of course, even more important is that you can have confidence your infrastructure is safe from attack and your organization will be free of the hefty non-compliance related fines that could come from unpatched software.

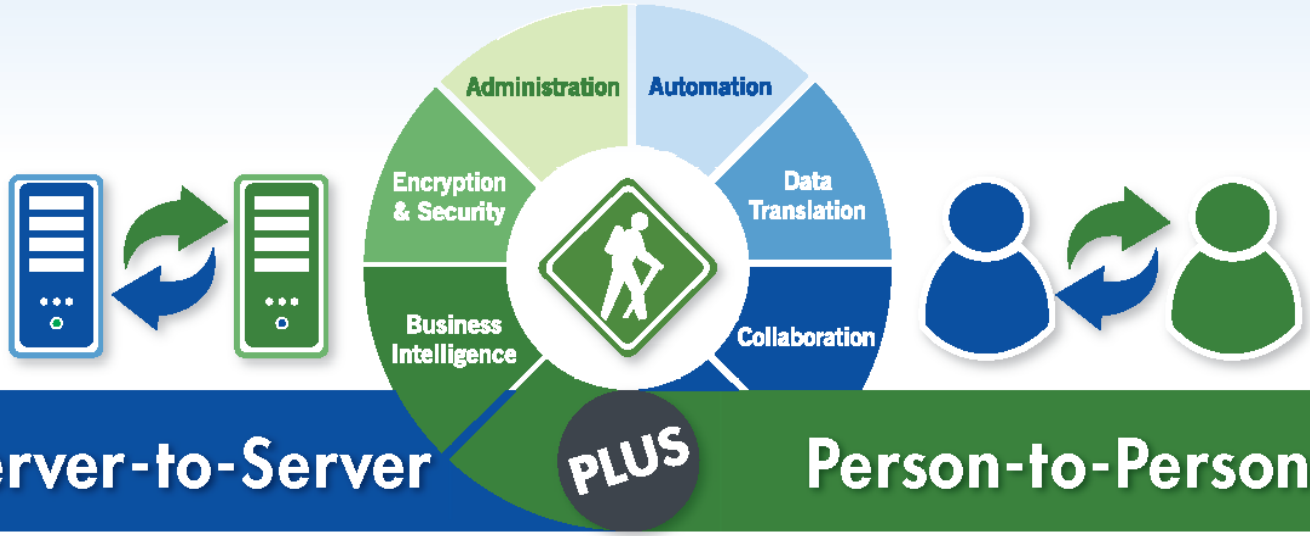
And if you're wondering how to best tackle these steps, remember that patch management tools can help automate them, relieving the burden on you to carry out each step manually.

About the Author

Naren Vaideeswaran, Product Marketing Manager, Security, SolarWinds

Naren Vaideeswaran is a product marketing manager at SolarWinds for the company's security portfolio. A technology enthusiast, he has worked in the IT and security industries for over a decade in both technical and marketing roles.

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

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

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

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

Visit GoAnywhere.com for a FREE trial.

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

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

One of the Largest North American Railroads

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

GoAnywhere.com 800.949.4696

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

Cyber Security Protection Requires Teamwork, Collaboration & Real Partnership

By Robert B. Dix, Jr., Vice President for Global Government Affairs and Public Policy, Juniper Networks

Recent high profile data breaches in government and industry provide compelling evidence of the growing cybersecurity challenge and its potential adverse impact on national and economic security globally. No longer are the risks limited to website defacements and nuisance hacking; or even identity theft and stealing credit card or bank account information; or even political hacktivists like Anonymous or others. Events like the OPM breach, Sony attack, Target compromise, and others vividly illustrate the growing capabilities and sophistication of criminals, nation states and even terrorist organizations.

Although the topic of cybersecurity has elevated across the public and private sectors, and the dialogue has driven greater awareness in Washington, DC, across the country and around the world, there remains a great deal of confusion about what to do to contain and address the evolving risk in cyberspace.

While it is important for Congress to pass meaningful legislation to improve cybersecurity information sharing and provide sufficient liability protection for entities that share sensitive information with the government, along with insuring appropriate privacy protections, there is much more that needs to be done quickly to address cybersecurity preparedness and resilience in the United States and around the world.

The Cybersecurity Information Sharing Act (CISA) of 2015 (S.754) is an important measure that will certainly address some of the current challenges to the exchange of relevant cybersecurity information between industry and government. However, it is important to note that information sharing itself is not new and, in fact, has been going on between industry and government as well as within and across industry for quite some time. The significant gap that remains and is largely unaddressed by CISA or any other current proposal is the ongoing reluctance of government to share timely and actionable cyber threat information and threat intelligence with the private sector.

That type of information, when available, is often withheld by government due to concerns about classification of the information. Some opine that too much information is classified and over-classified to the detriment of effective bi-directional information sharing. Importantly, such information is a key ingredient to protection, preparedness and resilience in cyberspace. Better understanding the tactics, techniques and procedure employed by the bad guys, along with the attendant analysis to determine what protective measures, had they been in place, might have prevented or reduced the impact of a cyber event is critical to making informed risk management decisions and investments. There are some who seem to believe that passage of CISA will solve the evolving and increasingly perilous cybersecurity challenge. While effective bi-directional information sharing is a critical element, it is but a tool to achieving the real objective, which is timely, reliable, and actionable situational awareness during steady state operations and throughout thresholds of incident escalation.

In order to actually achieve a sustained and productive national capability, we need to establish a credible early warning mechanism for cyber that relies on the ability not just to share information but also to correlate and analyze the information to identify patterns and trends of abnormal, anomalous, or even malicious behavior to prompt the issuance of alerts and warnings, and even recommended protective measures. Such information then would be shared with stakeholders broadly to raise awareness and provoke risk management actions.

Currently, too much effort, energy, and resources are spent on response and recovery. An operational capability with an early warning mechanism would allow the United States to improve detection, prevention, mitigation, and response to cyber events that may become incidents of national or even global consequence. By flipping the equation, not only do we improve our overall national cyber protection profile, but we also make it more difficult and more costly for the adversaries, no matter their level of sophistication.

This model is not without precedent. Through leveraging technology to gather, correlate, and analyze data streams related to climate and weather, the United States has been able to significantly improve the ability to predict serious weather events and by issuing early alerts and warnings, along with recommended protective measures, reduced the impact of such events and likely saved lives. Similarly, through leveraging technology to gather, correlate, and analyze health data streams with the appropriate privacy protections, the United States has been able to significantly improve the ability to predict serious health events such as measles outbreaks and the H1N1 virus, and by issuing early alerts and warnings, along with recommended protective measures, reduced the impact of such events and likely saved lives.

In the same way, the United States can create a comprehensive and sustained national capability to improve detection, prevention, mitigation, and response to cyber events that may become incidents of national or even global consequence by identifying patterns and trends of unusual, anomalous, or even malicious cyber activity that would prompt timely alerts and warnings and even recommended protective measures.

Accordingly, the improved sharing of threat indicators between industry and government, remembering that such indicators are not personal information but instead include items such as IP addresses and file hashes is an important step, but not the only step that is necessary to improve our ability to protect, defend, and respond to cyber events of national or even global consequence. Creating a truly functioning operational capability, not just the push and pull of information, but the necessary analysis to identify troubling behavior and issue early warnings to stakeholders is critical.

Lastly, there is another important information sharing step that does not require legislation and should be implemented immediately. When large scale cyber intrusions occur, the government is often engaged not just to assist with mitigation and remediation, but also from a role in law enforcement and investigation. Such a process will typically identify the tactics, techniques, and procedures utilized by the intruder, and may also identify what protective measures had they been in place might have reduced the impact or prevented the event altogether. An after-action report will often identify findings and recommendations resulting from the investigation.

Where and when appropriate, and without unnecessarily or inappropriately revealing or exposing proprietary information or other findings that may be classified or otherwise not appropriate for public dissemination, it would be useful to prepare an unclassified version of the after action report that would be a useful tool to practitioners across the stakeholder community and would include information about what tactics, techniques, and procedures were utilized by the adversary and what protective measures, had they been in place, might have prevented or reduced the impact of the event. Learning from real-life experience is a powerful tool to help inform cyber risk management plans and practices. Leveraging the tremendous capabilities of the FBI, Secret Service, and other components of the government to provide useful lessons learned to the stakeholder community would not only raise awareness, but also contribute to informing users and practitioners about priority approaches for managing risk across their own environments.

The 2015 CISA along with other pending legislative measures are important arrows in the quiver of cybersecurity protection and preparedness. Learning from the functional and operational capabilities utilized every day by the National Weather Service and the Centers for Disease Control, and applying those lessons to building a comprehensive and scalable national operational capability that will improve our collective capability to detect, prevent, mitigate, and respond to cyber events will enhance our national cyber protection profile and make it more difficult for the bad guys to achieve success. Combining these activities with a comprehensive and sustained national education and awareness, driven by public and private sector collaboration, to teach users how to better protect themselves in cyberspace, will improve cyber hygiene and raise the bar of cyber protection.

October is Cybersecurity Awareness Month and there will be even more attention by the media, policy makers, business leaders and more to raise awareness about cyber risk and our shared responsibility for assessing and managing that risk. Let us leverage that attention to produce more tangible and meaningful action. Working together in a collaborative manner among all stakeholders; public sector, private sector, academia, non-profits, and many more, we can make a difference in addressing the evolving cybersecurity challenge. Let's get to it…

About the Author

Bob Dix is Vice President for Global Government Affairs and Public Policy at Juniper Networks. He was Chair of the Partnership for Critical Infrastructure Security from 2011–2014 and chaired the Information Technology Sector Coordinating Council from 2008–2009. He has been an active industry leader in efforts to improve cybersecurity and critical infrastructure protection for more than 10 years. He served as Staff Director for the House Subcommittee on Technology & Information Policy during the 108th Congress.

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

BOOK NOW AT WWW.MEXICOSECURITYFORUM.COM

Sponsored by: CERBERUS CERTIFIED SECURITY PROFESSIONALS

Supported by: ALAPSI

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

Risk Acceptance Is A Key Factor To Next-Gen Security Strategies

Letting Reality, Not Perception, Drive Measurable Change

by Irena Mroz, SVP Marketing, Cryptzone

The continued prevalence of high profile security breaches remind us that today's public and private sector practices are not working.

Is access to technology to blame?
As we race to purchase the latest device and increase technology savvy, we rarely think about the malicious user who now has access to the same increased capabilities. With a computer, anyone anywhere can be a hacker.

Does that sound glamorous to the younger, idealist generation, or even the older, less in-demand veteran? The fact is, technology is user-agnostic: it doesn't care whether it's being used for good or evil.

Risk acceptance is part of our changing world.
It's human nature to avoid acknowledging risk and deal with it head-on, but the damage that can result from a security breach can no longer be ignored. Furthermore, everyone needs to be accountable.

Consumers shouldn't assume their data is being protected. Companies must take whatever precautions necessary to thwart an internal/external invasion.

People have too much access to information, most of which they don't need.
Assigning user access permissions, identifying a company's critical data and enacting monitoring tools are steps in the right direction to establishing successful security practices.

I recently met with a security guru from the government sector who suggested the following approach: strip every employee of access to everything and make them lobby for only the data they need to effectively do their job, and grant monitored access from there.

It sounds extreme, but makes sense. If you know who has access to what information, why they have access, when they should access it and for how long, you can accurately track normal behavioral patterns and anomalies.

It's not just about protection and detection, but ongoing security management.
Securing data is an endless loop of establishing controls, testing/monitoring, evaluating success and making adjustments. Institute defense in depth layers.

Encrypt sensitive or regulated data. Patch all systems, workstations, servers, endpoints, *etc.* throughout the supply chain, and keep them current with updates and baseline standards.

Risk acceptance includes identifying suspicious internal people/factors.
Don't underestimate internal threats. Legacy systems requiring unique security measures are accompanied by legacy people who are resistant to change.

Possessive employees that impede proper authorizations/protocols raise a red flag. IT execs that transfer responsibility to the cloud storage team and don't maintain the same commitment level to security are a detriment. Those conducting "shadow IT" initiatives are a danger…

Acknowledge risk and accept the reality of breach. Only then can an organization properly plan its next-gen security strategy.

About The Author

Irena Mroz is the Senior Vice President of Marketing for Cryptzone, a provider of dynamic, context-aware network, application and content security solutions. Mroz leads the security company's strategic direction and execution of global marketing and communications initiatives.

With more than 20 years as a technology marketing executive, her previous roles include senior positions at Bottomline Technologies and Create!form International.

A graduate of Boston University's College of Communication, she is an advocate for social responsibility throughout her many industry and volunteer affiliations. Mroz can be reached at irena.mroz@cryptzone.com, LinkedIn and at www.cryptzone.com.

The 12 Worst Network Security Practices Part 2 – Say no to the 'Culture of No'

By: Ofer Or, VP of Products at Tufin

We began this blog series discussing the mistake IT professionals tend to make in falling for a 'shiny new object,' aka the latest and greatest technological innovation. This time, we're honing in on what Gartner considers to be the *second* 'worst practice' when it comes to network security: the 'culture of no.'

This type of culture refers to many things, however Gartner is referring to the countless security departments that "do not enable their end users to quickly embrace new technologies." This may seem to contradict the idea around avoiding 'shiny new objects,' and that's because it does – in a way.

Nothing good ever comes from extremism of any kind, which is why there needs to be a happy medium between purchasing and adopting every new technology that hits the market, and simply refusing to evolve with the rest of the IT world. Furthermore, some users reported that they strongly believe "security departments implement policies and controls without regard for business function."

A common example of this disregard is when CISOs block employee access to a specific resource such as a website, server or application without a true understanding of who uses this resource, the purpose of the resource, or the business implications of blocking this access.

Another instance Gartner cites is forced patches upon employees' devices while not providing an option to bypass or delay these updates.

Turns out, security professionals' for the most part agree with Gartner from this standpoint. In a recent study by ESG Group, one of the top security challenges (cited by 39% of respondents) is that "IT initiatives are being adopted without the proper network security oversight or controls in place".

A similar study by RSA and ISACA found that the #1 skill gap for security professionals is the ability to understand the business side of things. Basically, security professionals don't understand how the business operations work, and therefore make decisions that impact the business without understanding the full implications.

And yet another comparable statistic for this can be found in a NetworkWorld survey, in which 60% of respondents stated they don't feel confident about their readiness to effectively deliver the applications and services that are their organizations' top priorities.

Basically, business leaders are making decisions on behalf of the entire organization without a proper understanding of the security implications, and security leaders are making decisions without a comprehensive understanding of the potential impact on the business. It's a classic case of miscommunication, which can be the key to disaster in an organization.

It's time that both sides of the organization – business operations and security – begin a very important conversation to align their needs.

If there is an imbalance or lack of compromise, you increase your organization's overall risk of failure by creating a subculture of Shadow IT – basically technology used without explicit approval to do so. Without unified IT management, there is no room for collaboration, not to mention increased security risks.

There needs to be that call-to-action to both security professionals – who must define the necessary security policies, controls and best practices, and business leaders – who need to provide full visibility into the critical business applications that will be affected by said policies and controls. Similarly, application owners should shape their applications with security in mind at the beginning design stages.

A simple solution to the 'culture of no' is the enterprise's adoption of successful security policy orchestration. This type of system provides a centralized, application-driven insight into an organization's network, which allows clear communication of the possible business impacts of alterations made to security controls prior to actually making the alteration.

In tandem, this would permit application owners to openly share their networking requirements and supply the IT leaders with direct visibility into the security and compliance effects of these applications. Adopt a 'culture of yes!' That way both parties can freely and effectively collaborate to achieve the best of both worlds – security and business agility.

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.

THE NO.1 INTERNATIONAL EXHIBITION FOR NATIONAL SECURITY AND RESILIENCE IN THE MENA REGION

ISNR

INTERNATIONAL EXHIBITION FOR NATIONAL SECURITY & RESILIENCE

15-17 MARCH 2016

ADNEC, ABU DHABI, U.A.E

www.isnrabudhabi.com

CROWD MANAGEMENT

THE FUTURE OF POLICING

DISASTER PREVENTION

INFOSECURITY

BRINGING GOVERNMENTS, BUSINESS AND INNOVATION TOGETHER FOR A SAFER WORLD.

PLANNING FOR FUTURE GROWTH AND SUCCESS IN 2016

18,000 ATTENDEES

200+ GOVERNMENT BUYERS AND DELEGATIONS

500+ EXHIBITORS

90+ PARTICIPATING COUNTRIES

SOLUTIONS FOR AN UNPREDICTABLE WORLD

As the Middle East's leading biennial event specialising in homeland security and national resilience, ISNR 2016 offers governments, security and emergency services a unique opportunity to source innovative technologies along with a chance to learn the latest strategies to prepare for, protect against, respond to and to recover from a world of hazards. For the world's leading security suppliers, it means a unique opportunity to talk direct to government buyers, make new contacts and secure new business opportunities.

BOOK YOUR STAND TODAY!

NEHME SHEHAB - Group Sales Director ▪ **Tel.:** +971 2 409 0346 ▪ **E-mail:** nehme.shehab@reedexpo.ae

Platinum sponsor

Featuring

Co-located events

Organised by

abudhabipolice
@abudhabipolice
theabudhabipolice
moiuae

Data Breaches, Cybersecurity, and the New Normal

By Scott M. Higgins, CISA, CRISC, CRMA, Director, WeiserMazars LLP
& Moises Brito, CPA, CISA, CIPP/US, Manager, WeiserMazars LLP

During the first nine months of 2015, organizations from a range of industries have been affected by cybersecurity breaches. Just a few of the more famous victims include Anthem Inc., The Internal Revenue Service (IRS), British Airways, and Ashleymadison.com.

These organizations all have one thing in common - each possesses valuable consumer data such as names, addresses, credit card numbers, financial institution information, protected health information, and social security information. In the face of these ongoing threats, it is vital for businesses of all kinds to have a strategic plan to safeguard their operations.

"This is the new normal," says S. Gregory Boyd, Partner and Chairman of the Interactive Entertainment Group at Frankfurt Kurnit Klein & Selz. "Especially for media companies. We're seeing regular breaches across the industry both generally and in response to stories, movies, or other products that an individual or country doesn't like. All organizations need to be ready for cybersecurity breaches and do what they can to protect themselves."

An Effective Strategy

The first step when developing a cybersecurity strategy is to perform a risk assessment. The goal is to identify security vulnerabilities involving the transaction and storage of sensitive information, and then allocate resources for protecting that data commensurate with the level of risk involved.

A risk assessment should be performed for each unique application, and the related infrastructure, that performs transactions and stores data.

Each risk assessment should begin with a detailed understanding of all business use of data and surrounding controls, and include all outsource areas such as, payroll, asset custody, or claims processing.

The result of an effective assessment will be determining which data is worth protecting (including personal information of customers and employees, and confidential business and development plans), and a clear vision of how to improve security to better protect it.

Says Justin Berman, VP of Information Security at Flatiron Health, "It's important to really understand what you are actually protecting. It's easy to assume that we are all protecting the same thing, but the truth is that protecting a hedge fund is different than protecting a health care organization.

There are different areas that need attention and different approaches that need to be taken based on the organization's specific data profile."

How Operations Affect Cybersecurity

The operations of each organization have a significant impact on cybersecurity posture. Personnel, processes and technologies must all work together to protect the organization's assets.

Personnel

Organizations should strive to recruit individuals at all levels who have a fundamental understanding of common security practices. About 29% of breaches that occurred in 2014 were caused by employee-related errors.

Regular training sessions and periodic recertification of security requirements should be offered, backed by policies such as "clean desk" and daily shredding to make sure printed information with confidential data is not leaked.

Cybersecurity personnel should have a deep knowledge of best practices including those established by the National Institute of Standards and Technology (NIST), the Information Systems Audit and Control Association, (ISACA) and SANS Institute (SANS).

Employers should institute sound hiring practices such as background and reference checks for all security personnel, and arrange a demonstration of their skills.

Depending on the company's structure and size, it can be worthwhile to put in place an independent Chief Information Security Officer (CISO) and dedicated staff responsible for ensuring technology and information assets are adequately protected. Outsourcing of the function is possible, but a clear understanding of vendor management risk is essential.

Leveraging Processes

Day-to-day processes have a tremendous impact on the cybersecurity posture of a company. Controls should be deployed that are automated and preventive to minimize information and cybersecurity-related risks.

As companies grow, many rely on detective controls to manage their operations, usually through the IT department. For example, about 43% of organizations surveyed say that they still manually review logs.

The manual review of logs is a difficult and sometimes incomplete process. It is a better use of security personnel to design and implement preventive controls and real-time monitoring techniques and processes in cooperation with Compliance and Internal Audit.

Along with other measures such as: adequate review of personnel; disabling USB ports on PCs; and automated scanning of emails for sensitive or confidential information, these improved processes will decrease the likelihood of data leakage.

Strengthening IT controls can also increase the efficiency of other business functions – a win/win.

Implementing Technology

Consistent patching, penetration exercises and vulnerability management is part of a well-run IT department. IT departments should also vet new technologies for any risks that they may introduce to the current organizational environment. Common industry practices should be used at all levels, such as encryption during data movement and at rest.

Cloud computing introduces additional security risks because of the greater dependency on third parties, increased reliance on independent assurance processes, and use of the internet as the primary conduit to the organization's data. If a company uses a cloud solution, they should thoroughly assess the risks associated with public and private clouds.

Incident Response

Depending on the data that an organization holds, it may be subject to attacks hundreds of times a day. If a breach happens, a well-executed incident response plan can mean the difference between additional data loss or finding the source.

Companies should have an incident response team with pre-established policies and procedures that are compliant with the breach notification laws of each state where business is done or sensitive data stored. The team should be made up of people from different functional areas so that every group that may be affected by a breach has first-hand knowledge of what's going on.

Incident response procedures should have step by step guidance for declaring, reporting, and containing a breach. Additional forensic information may also need to be included, depending on applicable laws. Law enforcement personnel should not be contacted until the organization's legal counsel has authorized its involvement. If malicious intent is suspected, however, this may be the best course of action. Law enforcement personnel can help internal teams determine the scope of the breach and if a similar breach has been experienced at other businesses. After affected assets have been removed from the system, a full forensic audit of the company's records and any recordings of the events that led to the breach should be conducted. Employee communication is critical during a breach - the more knowledge employees have about what happened, the more likely they are to comply with existing controls, and may recommend new controls that should be in place.

CyberSecurity & ERM

The Department of Homeland Security's Cyber Risk Management Primer for CEOs describes key cyber risk management concepts:

1) Incorporate cyber risks into existing risk management and governance processes.
2) Begin cyber risk management discussions with your leadership team.
3) Implement industry standards and best practices. Don't rely on compliance.
4) Evaluate and manage specific cyber risks.
5) Provide oversight and review.
6) Develop and test incident response plans and procedures.
7) Coordinate cyber incident response planning across the enterprise.

8) Maintain awareness of cyber threats.

"Many people, even top-level management, don't include cybersecurity in their ERM," notes Nicolas Quairel, Partner and head of IT Consulting at WeiserMazars LLP. "They don't include it because they don't see where it fits in the traditional structure.

But the truth is that cybersecurity risks are very serious and need to be included in any comprehensive ERM program. There is a direct connection between technology risk and business risk."

It has become increasingly important to treat cybersecurity risk as any other business risk, including considering it in the Enterprise Risk Management (ERM) program. Cybersecurity's deep impact on consumer perception, the overall business, and revenue, make it an organizational risk, not just an IT risk.

Recent guidance from COSO explained how its 2013 framework and 2004 Enterprise Risk Management, Integrated Framework can help companies evaluate and respond to cybersecurity risks.

Barriers to Getting Started

Often times finding the right individuals and establishing knowledgeable committees make treating cybersecurity with appropriate seriousness a major challenge.

A strategic vision and process must be developed, including designating who is responsible for cybersecurity and information systems at the C-suite level, such as an independent CISO.

Risk committees and measurement programs should also be put in place to evaluate inherent and residual cyber risks, and to incentivize and track the progress made in these areas.

As cybersecurity risks become more complex, the longer organizations take to adapt to the new landscape makes it more likely that sensitive and confidential data will be compromised.

Sources

http://www.sans.org/reading-room/whitepapers/analyst/data-center-server-security-survey-2014-35567

https://www.promisec.com/blog/study-shows-data-breaches-due-to-employee-error/

http://www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

http://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf

http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

About the Authors

SCOTT M. HIGGINS, CISA, CRISC, CRMA

Scott has over 30 years of industry and advisory services experience, providing a unique combination of capabilities in compliance (internal audit, Sarbanes-Oxley, NAIC Model Audit Rule), operations (business process transformation, operational effectiveness), technical (Information Technology), and managerial (budgeting, forecasting, human capital development).

Scott's major areas of focus include overseeing all Information Technology (IT) external Audit support, Service Organization Control (SOC) reports, IT due diligence, IT Internal Audit, as well as other IT consulting including IT assurance services. Scott has led internal audit co-source engagements in a number of industries (health care and

P&C insurance, REIT, financial services, manufacturing, distribution, service), providing financial monitoring and business process effectiveness, as well as managing extensive portfolios of risk-based assessments including business process transformation, IT strategy and governance, system development life cycle, change management, network security, telecommunication security, and vendor audits. Scott holds a BS in Computer Science from DeSales University, an MBA from Moravian College, and a Masters Certificate in Project Management from Stevens Institute of Technology. He is a Certified Information Systems Auditor (CISA); is Certified in Risk and Information Systems Control (CRISC) designations by ISACA; and is Certified in Risk Management Assurance (CRMA) by the IIA.

CONTACT

WeiserMazars LLP
Scott M. Higgins | Director
501 Office Center Drive, Suite 300
Fort Washington, PA 19034

(P) 267.532.4325
(Email) Scott.Higgins@WeiserMazars.com

MOISES BRITO, CPA, CISA, CIPP/US

Moises has spent over six years providing consulting, project management and audit services to a range of clients in the technology, retail, financial services, health care, higher education, real estate and not-for-profit sectors. He performs IT effectiveness reviews, control design, systems development, change and logical access management, disaster recovery, Payment Card Industry (PCI) assessments, and statement on controls (SOC) I and II including Privacy Assurance and Maturity, as well as vulnerability, penetration, social engineering and cyber security enhancement studies. These reviews include inspecting technical IT databases such as Oracle, MySQL, DB2, middleware and evaluating the

weaknesses involved in the processes and the technology used. Moises has extensive experience in SAP, Oracle and JD Edwards accounting information systems. Through his insight and identification of IT vulnerabilities, Moises's clients have significantly benefited from a stronger IT environment.

Moises has a deep background in assessing privacy maturity programs, designing controls and performing compliance audits. He has conducted in-depth reviews of data localization to assist companies in understanding their privacy posture.

Moises also has niche experience helping with COBIT, NIST, AICPA Privacy Principles, SANS institute and ISO Security frameworks for cyber security technology and techniques.

Moises helps middle-market clients implement the effective IT risk assessments needed to allocate resources to meet compliance requirements. He has also designed and tested SOX 404 key controls.

Moises received his Bachelor of Science degrees in Accounting and Information Systems from King's College. He is a Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA) and a Certified Information Privacy Professional (CIPP/US).

CONTACT

WeiserMazars LLP

Moises Brito | Manager

135 West 50th Street

New York, NY 10020

(P) +1.212.375.6832

(Email) Moises.Brito@WeiserMazars.com

Innovation and Security Need a Community

By Lenley Hensarling, Vice President, Strategy and Product Management, EnterpriseDB

The maelstrom of controversy in the wake of the now famous blog from Oracle's Chief Security demonstrate a certain tension between Oracle and its customers. She raised several valid points, such as the need to comply with contractual commitments around reverse engineering source code.

But the tone of her post, and other posts called out in the media, was belligerent toward Oracle customers.

The language didn't carry the sense that, in this world of internet-connected applications and infrastructure, the vendor and customer are in it together, by necessity, and in point of fact.

If companies using technology and companies producing technology are to succeed in doing their best to provide security in an increasingly insecure world, there has to be a sense of cooperation.

One reason for this is that security is not only rendered in the software, but also in how it is deployed and there is a reflexive relationship between the two in achieving the most secure solution. It is also impossible for a vendor to understand and anticipate every possible way their software will be deployed.

Customers need to understand the software, and transparency about how it works is a key part of that. In the open source world, customers can gain that transparency to virtually any level, dependent only on their desire and commitment.

They have access not only to documentation, but also to the source code, which is the ultimate truth about any software.

The interplay between those using the software and those making the software is made closer in the open source model. That leads to innovation through cooperation.

Open source contributors are typically users themselves and are focused on making the software better. Leadership is responsive when users identify vulnerability.

The Postgres Community manages security issues in a disciplined manner, when they do arise. Postgres, in fact, has a reputation for being the most secure open source database.

The Community publicly reports and repairs security issues primarily through the Common Vulnerabilities and Exposures organization.

Anyone can access the 'Security' link on the PostgreSQL.org home page to report or view security issues. Try searching http://cve.mitre.org/ for 'PostgreSQL.'

The community also works cooperatively with 'packagers' of PostgreSQL, like EDB and other

companies with ties to Postgres, to expedite patches to their respective user bases.

The key point here is that the interplay and cooperation between vendors, open source community members, and end users enables innovation in new ways. Many of the individual players flow across organizational lines.

End users of a given open source distribution may make contributions to the technology. Vendors' employees may drive the technology forward based upon customer input and make their own contributions to the code.

It is because of the spirit of a shared ownership of the technology and of the responsibilities, that when a customer or a contributing member of the community brings up an issue, it is taken on its merits.

Contributions are what drives open source, and they take many forms, from contributions of code but also contributions of finding issues and identifying vulnerabilities.

One of the valuable attributes of open source solutions is that they are by their nature more transparent, and therefore it is easier for end users to work in cooperation with vendors, for vendors to work together as partners and for the community to move the technology forward.

It takes a community, not just one company, to innovate and to keep things secure.

About the Author

As vice president of strategy and product management, Lenley Hensarling plays a major role in setting EDB's strategic direction through product development and customer and partner interactions. A longtime J.D. Edwards executive, Hensarling went on to leadership roles at PeopleSoft then Oracle.

His roots are in engineering and he quickly rose to vice president of engineering at Novell. Lenley has more than two decades of experience in the software industry in large enterprise technology organizations.

Algorithm-based Software vs. Algorithm-based Hardware

By Milica Djekic

Many encryption algorithms may be stored as both – software and hardware solutions. Whatever you hold as a software or hardware could be at risk once bad guys decide to deal with your effort. So, what would be more secure – to keep your confidential algorithm as your software or on your hardware? The both techniques got their pluses and minuses and right here we would discuss how all of them could be manifested. There is no a universal answer to this question, but rather an opportunity to estimate on your own as well as choose the most suitable solution to your organization at that certain moment.

The requirements for confidential algorithm storage

The main requirement for confidential algorithm storage would include a certain level of security in terms of reliable protection of content. As it's known, there is no an absolute security and nearly every – either software or hardware content – could be hacked, at least in a theory.

Confidential algorithm should as its name suggests deal with highly confidential or at least secret data and, in such a manner; we would assume it's correlated with some sort of encryption solution. It's clear that such a solution seeks a quite good level of protection and cannot be stored at a fully unprotected machine or device.

Nothing can offer to us an absolute security, but what we could try to do is to manage such a risk at an acceptable level. Theoretically, everything could be hackable, but it requires a certain amount of time and effort to take advantage over that resource.

For instance, if you hold a highly confidential encryption algorithm as software on a completely unprotected computer, you deal with a risk that someone could break into your machine and steal, change or destroy your product. Similarly, you could keep your cryptographic algorithm on some physical device as hardware-based solution and even, in such a case, your effort could be vulnerable to hacker's attacks.

Right here, we plan to provide a brief overview of possibilities offered by both – algorithm-based software and algorithm-based hardware as well as discuss good and bad sides of these technologies.

What could algorithm-based software offer to you?

When we try to compare a cryptographic algorithm produced as software with the similar solution given as hardware – at a first glance, we would notice that there is a difference in cost. Practically, it may be much cheaper to code your solution in some programming language, rather than to pack it into many ICs, diodes or transistors. So, software-based solution may appear as somehow cost-effective.

The next question we should deal with here is how secure such a solution is. If you develop a highly confidential algorithm and embed it into software, you would realize so soon that if your computer is

not protected well-enough – your masterwork can easily leak out from your machine. The disadvantages with this are that your brilliantly designed solution could get available on the black market without any difficulties.

Also, if you hold your source code on your machine, a hacker could try to change it through a carefully planned attack and consequently cause the permanent changes to your solution. On the other hand, there is a possibility that such a malicious actor could try to delete or even destroy your software using some malware.

Finally, your algorithm-based software may seem as somehow cost-effective, but is that the case for real? If we take into consideration how non-difficult it can be to break into someone's machine and take whatever you want to, it appears that this solution is still correlated with a risk that is challenging to be managed.

The pluses and minuses of algorithm-based hardware

The first assumption that we could apply here is – algorithm-based hardware got much higher investment costs than its software-based solution. This is accurate at a first stage only, but, in long-terms, such a solution still appears as much secure. Well, does it mean that algorithm-based hardware is so resistive to hacker's attacks?

Basically, this is not the fact and even this sort of effort has its good and bad sides. Firstly, we would agree that it's much harder to steal algorithm stored on hardware, rather than as software. You would realize that to get your hardware solution, you must be physically present at a scene which is much challenging than, say, so easy breaking into someone's computer from a proper distance. In addition, in order to extract algorithm from your hardware, you need an appropriate technology which is somehow difficult to develop.

At the end, as these sorts of algorithm-based hardware are usually stored as some types of external devices connected to your computer, it's clear that this solution could be compromised using some malware that could damage or completely destroy such an effort. So, a 100% of security is not promised here at all!

Some concluding remarks

As we would see this topic as extremely interesting, we would suggest this to get investigated deeper which could offer us to deal with much accurate and reliable details and analysis. We believe such an effort could be so useful for some future applications in this field.

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.

Thermal Imaging Smartphone Accessory Leaves Millions of cash Machine Users at Risk

Once The Sole Preserve of Only The Best-Equipped Attacker

by Dave Wray Principal Consultant at Sec-Tec

UK security consultancy firm Sec-Tec has warned consumers that a readily available smartphone accessory can be used to steal customers' PIN numbers within seconds.

The thermal imaging device is worryingly being sold across the Internet as an iPhone accessory costing less than £200. Once the sole preserve of the best-equipped spies in blockbuster movies, the technology has created an increased risk for millions of push-button security devices from door entry systems to safes.

The device has its advantages for criminals, as traditional ATM fraudsters are often impeded by customers blocking the keypad with their hand, making the skimmed data more or less useless. With this new accessory, the heat from a person's fingertips can leave a heat trace on the keypad for around a minute.

But while identifying the keys pressed is straightforward, knowing the order in which they were pressed is considerably more difficult for fraudsters. However, the security firm has created various undisclosed methods that considerably aid the identification of key ordering, although most keypad devices have no lock-out mechanism; meaning that only a set number of possible combinations of the four digit code are correct.

Sec-Tec has identified two simple techniques that anyone can implement to stop the device successfully recording the heat trace – namely, using a metal object such as a key to press the buttons, or rubbing the full keypad as a way of 'erasing' the trace history .

"The thermal imaging device exposes millions of push button locks & ATMs around the world as the digital security arms race gets ever more sophisticated" said David Wray, Principal Consultant at Sec-Tec.

About The Author

Dave Wray is the Principal Consultant at London-based security consultancy, Sec-Tec ltd. The company was formed in 1999 and provides penetration testing and vendor independent information security services to a wide range of public and private sector clients including global law firms and FTSE 250 financials. Our vendor agnostic approach enables the objective delivery of security services without any hidden agenda. Sec-Tec is currently ISO9001 and ISO27001 certified and employs Tigerscheme (http://www.tigerscheme.org/) certified staff.

Dave Wray can be reached online at the company website https://www.sec-tec.co.uk/

EXHIBIT IN 2016

SSS
Saudi Safety & Security
2016

Saudi Arabia's leading security, fire and safety exhibition

16 - 18 May 2016
Dhahran International Exhibitions Center,
Dammam,
Kingdom of Saudi Arabia

The SSS 2016 international exhibition will play host to innovative and pioneering technologies and products aimed at overcoming security, safety and fire issues. Saudi Arabia is now one of the world's fastest growing markets for security and safety solutions, making the SSS 2016 exhibition an ample opportunity for companies to network with private companies offering solutions in the fire, safety and security space.

> "A great launchpad for getting collaborators/prospects/potential clients in the Middle East region together. The perfect event for safety professionals."
>
> Neclilae Edcuard,
> Marketing Manager, Invictus (Adina SRL)

2015 PARTICIPANTS

Want to exhibit?

Please contact Mostapha Khalil E: mostapha@bme-global.com T: +44 203 463 1097

Previous Supporters

2015 Sponsors

Official CPD Member

Organised by

Official Production House

Official Housing Agent

2016 Media Partners

www.sss-arabia.com

Follow us on Twitter: @bmeevents
For all the latest news: @SSS_Arabia #SAUDISECURITY2016

How Cloud Computing Willing Change The Future

Cloud computing already has changed the way we think and live, but even more changes await us as new systems and technologies make us less dependent on traditional computing devices and more dependent on interconnected global networks.

Composed of off-premises infrastructure and software resources, has already untethered many of us from our desks, allowing us to reach unprecedented productivity levels, even when mobile.

Although many cloud resources have already become staples of modern life, even more changes await.

Cloud computing is in its very infancy and already it is reshaping the way things work and creating new industries.

A thriving middle man industry is already bridging the gaps between technical wizardy and the layman.

The following are just a few ways cloud computing will change the future.

Health Care

Thanks to the ubiquitous cloud, home-based health monitoring systems will continue enhancing medical care.

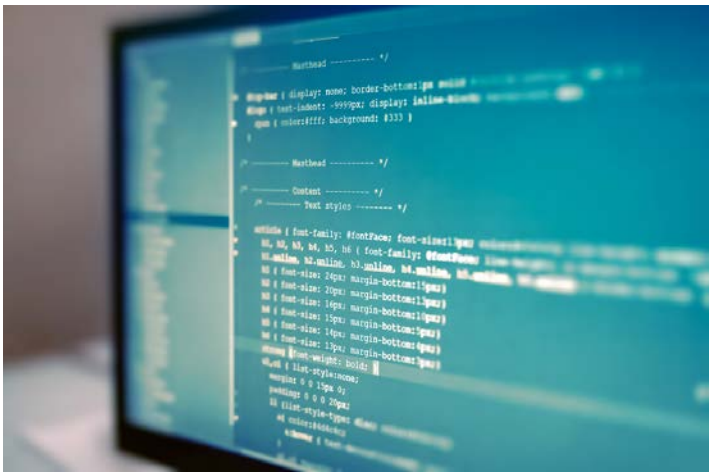
Everything from heart rates to sleep can be monitored remotely, in real time, reducing the need for visits to the doctor.

Beyond monitoring, cloud computing will enable robust diagnostic equipment, once limited to large medical centers, to be available in small medical practices, using the cloud for the necessary computing power.

We should also look for an increasing number of virtual house calls, performed by physicians.

This trend allows patients to visit with a doctor via a video call, eliminating the trip to the doctor and paving the way for virtual consultations with specialists and other medical professionals.

Software



Software applications will continue to move to the cloud as developers work to marginalize hackers and improve services.

The cloud-based software model can utilize cloud-based computing power to make applications run faster on thin clients and mobile platforms without sacrificing features.

This has opened up entirely new business niches. A CRM (Customer Relationship Management) is pioneered by Salesforce but it if you check out CRM reviews on the web you will find an entire industry of CRM platforms.

Cloud computing makes these types of platforms and services have sustainable margins where as before hardware costs would have made these types of services a no - go.

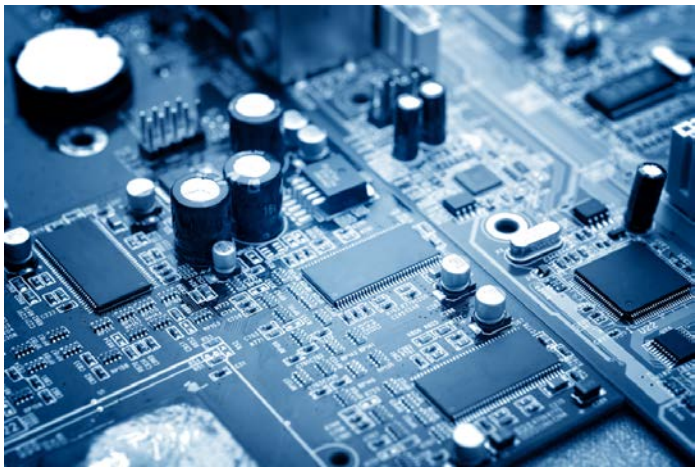
Licensing and software updates will continue to be cloud-based, enhancing security while improving performance and speeding the delivery of innovations.

Ultimately, software applications will become independent of hardware, delivering a consistent experience anywhere on the globe.

Commodity Hardware

With low-power, high-speed, 64-bit processors on the horizon, Cloud Computing will commoditize hardware to a new level.

Hardware interfaces to the cloud are expected to become inexpensive and interchangeable, simplifying data centers and paving the way for software intelligence and automation.



Paradigm Changes

A new breed of IT professionals will soon come of age, bringing new paradigms with them.

These will be people who grew up with the Internet and are comfortable accepting hardware and software as services, rather than as discrete entities. This new generation will provide the impetus needed to change completely the way people and corporations interact with the cloud.

Workplace Transformation

Many experts speculate the cubicle will soon become extinct as a mobile, connected workforce begins to work from almost anywhere.

Life will dominate work, especially as traditional jobs disappear.

Similarly, in the new workplace, information silos will no longer be a factor on the job, as information and expertise become accessible to everyone.

The coming surge in productivity might mean people work for their profession, serving numerous companies and eliminating office politics.

Security Will Change

As cloud computing continues to grow home and business security will change. Gone are the days when large video databases were needed to store security footage.

Services such as IP Camera Hosting are quickly becoming popular. These services cut down on cost, maintenance, and the need for personnel, they are quickly changing the security industry.

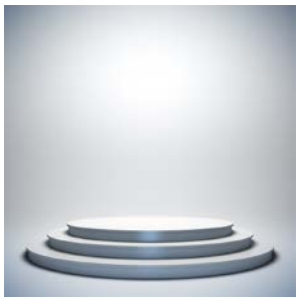
The Machine Age

Soon, the Internet will boast more than one trillion connected devices. People will grow accustomed to their presence, as the number of computing of devices continues to rise, they will require less human interaction as almost every routine task becomes automated. The number of devices will continue to grow as the cost of devices plummets. Fueled by expected increases in IT, the explosive growth of cloud-connecting devices will provide for unprecedented levels of automation and innovation.

Legacy Headaches

As the cloud becomes increasingly pervasive, IT professionals will face a growing challenge as they deal with obsolete equipment. The cost of managing legacy systems could become overwhelming for businesses trying to compete in a new environment. Managers will quickly need to replace aging systems, so their companies can compete in the cloud.

Platform as a Service



As software developers work to keep up with the changing IT landscape, companies will increasingly turn to either internal divisions or external companies to provide platform services. Software developers will no longer spend time creating applications to manage elasticity and scalability. Instead, Platforms as a Service (PaaS) providers will deploy platforms that conform to the software. Cloud computing has changed our behavior in ways we could not have predicted, even just a short while ago. Although the future promises to be as unpredictable as ever, we know that the businesses and workers that will quickly adapt will also thrive.

About the Author

Lee Ying has over 10 years experience in the tech and security industry. He currently writes for various websites, if you would like to contact him you can find him on LinkedIn: https://www.linkedin.com/pub/lee-ying/9a/18b/238. Follow me on Twitter @LeeYing101

A Must Attend Event For All Senior Level Information and Cyber Security Executives

CYBER SECURITY SUMMIT 2015

Official Title Sponsor paloalto NETWORKS

Attend the Cyber Security Summit

These Invitation-Only events connect Senior Level Executives with the world's leading Cyber Solution Providers and Thought Leaders.

New York City
September 18
Millennium Broadway Hotel

Boston
October 21
Back Bay Events Center

Register Today for **50% OFF** Full Summit Passes using Promo Code: **CDM2015**

Partial List of Solution Providers

Intel Security • Symantec • Trend Micro • Darktrace • Verisign • WatchGuard Technologies • Checkmarx
SurfWatch Labs • SGA Cyber Security • HillCrest Agency • Exodus Intelligence • eMazzanti • HillCrest Agency
Deep Node • Covata USA • CenturyLink • AlgoSec • Vectra Networks • Akana • EnSilo • RedVector
Bit9 + Carbon Black • Illusive Networks • Terranova Corporation • Varonis Systems • Vectra Networks

For Business Development Opportunities Contact Bradford Rand at
212.655.4505 ext 223 or **BRand@TechExpoUSA.com**

www.CyberSummitUSA.com

Ransomware hacks Android's front-facing camera to take embarrassing photos

An Android app that offers pornographic images, Adult Player, has been recently discovered to be a particularly aggressive form of ransomware.

The malware secretly takes photos of the unsuspecting victim by accessing the device's front-facing camera and then locks it, demanding a $500 ransom while pretending to be affiliated with the FBI.

The FBI probably isn't after you

Unfortunately, as cyber criminals advance their tactics and techniques, the rest of us have to learn to catch up. Ransomware, which has been around for about as long as the PC, is now targeting Androids and other devices.

One of the major scare tactics of ransomware is to catch you in a compromised position, or a fabricate one, and threaten your sense of security in addition to locking your device.

That's often times why "FBI" will pop up in the extortion image that follows infection.

Earlier this year, an app named Porn Droid locked devices and accused the user of accessing child pornography, then demanded $500 as a penalty.

Similarly, the app Koler intimidated Android-using victims in the same fashion, and was contracted on pornography websites under the guise of a legitimate app.

The difference with Adult Player is that it can actually take embarrassing photos of you that wouldn't exist otherwise. And even if you do pay the penalty, who is to say that those photos will actually be destroyed?

Be selective about your downloads

Adult Player, as with many ransomware apps, is not available through Google Play. Often times these malicious apps can be found for direct download through a website, so it's best to avoid these kinds of downloads unless you have good reason to trust the company behind the app.

Additionally, you should always pay attention to what permissions you grant when you download any app.

If an app wants access to your contacts or camera, for example, and it should have no use for those functions, abort the download immediately.

How to remove Android ransomware

While this alert might give some of you a few laughs, it might make another handful of you blush in embarrassment.

If you've contracted the Adult Player ransomware, follow the steps below to remove it from your device:

1. Enter safe mode on your device. As there are different methods depending on your device, you might need to do a quick search online, here is one that works for most models.
2. Go to Security under Settings, and then select Device Administrator. Select the offending app and deactivate it.
3. Go to Apps, under Settings, and select Uninstall to remove the ransomware app.

Hopefully you have not downloaded Adult Player or any other ransomware for that matter.

But in the case that you have, remove it and remember in the future to focus on prevention over cleaning!

Have a great, ransomware-free day!

About the Author

Christian Mairoll Contributor, Emsisoft

Christian is founder and CEO of the Austrian anti-malware company Emsisoft.

For CDM, his aim is to educate our readers with essential security knowledge, especially in understanding and stopping new and innovative malware.

Solving The Cloud Security Puzzle

By Anthony Scotney, founder & CEO, StratoKey

Protecting cloud applications is a puzzle. The puzzle is complicated by all the moving pieces that expose yet another point of exploitation. But it is not unsolvable.

The secret to solving the cloud security puzzle comes down to a detail-oriented approach that focuses on visibility, user access interrogation, securing data before it reaches the cloud, and automated threat response.

Visibility

One of the great challenges with cloud and indeed web/SaaS deployed applications is the lack of visibility. Often Security Information and Event Management (SIEM) infrastructure has no access to logs of software provided as a service. This creates what is known as the SIEM blind spot.

Without visibility of how users are accessing end systems, organizations are at the mercy of third parties to determine their security outcomes, which is an unacceptable risk. Fortunately, there are solutions for uncloaking these SIEM blind spots.

Generally, the most effective way to gain insight and complete visibility is to lock cloud deployed applications to a security gateway. Users then transit through the gateway on their way to the cloud application.

This can take the form of a proxy server. As users transit through the gateway, significant security insight can be gained which can be added to the overall security picture for your applications.

User Access Interrogation

Often overlooked, User Access Interrogation is critically important for securing access to information. This is the leading reason why spear phishing and user credential theft is such an effective attack vector. Organizations are simply not doing enough to adequately interrogate users logging into their systems.

Non-hostile user interrogation (performed by technical analysis on the back-end) is key to securing access to confidential information. Currently, applications ask for a user's credentials (think drivers license) without ever looking at their face to confirm the identity. In many ways this is a result of the maturity cycle of the web.

Threat actors have caught onto this lack of identity verification but unfortunately the vast majority of infrastructure is still lagging behind.

It is possible to defeat user credential theft based attacks with appropriate technology, yet they remain a major cause of data breaches. Solutions to this security vulnerability can range from taking

machine fingerprints, geographical interrogation, second factor authentication and right through to detailed behavioral analysis.

Adding rigor to User Access Interrogation extends beyond the front door. Real-time user behavior analysis combined with automated threat response is key to defeating determined attackers. Using machine learning to understand how users work on a daily basis is crucial.

For an attacker to succeed they must then become the user, a difficult task without obvious means to extract significant volumes of confidential data.

Securing Data Before It Reaches the Cloud

Securing data means different things to different people. In the realm of cloud-deployed applications, it means protecting the confidential data used within the application. It is increasingly rare to hear about attacks on physical databases. It is not rare however to hear about attacks on applications exposing data stored in databases.

Securing your data at rest requires much more than database encryption. Database encryption is wonderful for securing the physical database. Unfortunately database encryption (by design) does not secure data when it is passed to the application for user consumption.

The security issue comes via the way that applications interact with databases. Applications are trusted users.

Databases give up the data to applications without the mandate to understand how this data is being consumed or indeed exposed.

Encrypting data before it reaches the application resolves this security weakness in system architecture. Having the data pass back through a separate encryption gateway that decrypts the data and makes it human readable is effective at securing the data against application attacks that bypass security gateways.

It would be neglectful to not mention that data needs to be protected whilst in transit. This in transit protection can come in the form Transport Layer Security (TLS). TLS encrypts the data in transit between users and the end cloud applications (SaaS and Web included).

This is network level encryption and provides no security once the data reaches the end application.

Automated Threat Response

There is questionable benefit of having the ability to detect attacks whilst lacking the tools to thwart them. Threat response is one of the toughest pieces of information security. There has to be a careful balance in all responses to ensure that legitimate users are not treated with an iron fist whilst going about their job.

Automating threat response is crucial to ensuring that threats are stopped without delay. Delays in threat mitigation can result in a data breach. Ignoring the warning signs whilst administrator's sleep can lead to catastrophic data breaches.

Additionally, alert fatigue can cause administrators to ignore the warning signs. Every administrator receives countless automated notifications from their security appliances.

There are well known data breaches that resulted in part due to alert fatigue. The potential catastrophic consequences of alert fatigue are a good reason to automate threat response.

Measured approaches to threats such as blocking requests, suspending user accounts or simply locking access for a pre-determined period may be all that it takes to defeat threats whilst limiting the potential for business interruption.

Summary

With more and more companies conducting business in the cloud, one would assume that all third-party application providers would make security their number one priority. But that is not necessarily the case.

As a result, businesses are being forced to take control of their own cloud security and make a best effort to protect their data and, ultimately, themselves.

The fact that the cloud is still relatively young and evolving makes solving the security puzzle complex, but the tools exist to secure a company's data in the cloud and protect businesses against data loss, leaks and breaches.

About The Author

Anthony Scotney is founder & CEO of StratoKey. StratoKey's intelligent cloud data protection is designed to address critical security vulnerabilities with cloud and SaaS applications. StratoKey utilizes encryption, behavioral analytics and strategic countermeasures to prevent data breaches. Anthony can be reached via www.stratokey.com.

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

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

The virus which will destroy your data

By Jean Lewis, Tech writer, Laptopical.com

Computer viruses take place in many different shapes, from the ones which attempt to steal our information to the ones which will actually delete all our precious data files. Every week sees the development of a new type of virus, which is why anti-virus programs are updated on a daily basis to counteract this very productive and ultimately damaging sector of the programming industry. This article will take a look at the virus called CryptoLocker which can destroy our data, making it very hard if not impossible to restore it to its original state.

Why are viruses created?

This is a question that is on a lot of people's minds. Indeed, why would a person create such program which only has negative consequences on people's daily digital lives?

The most common reason is similar to why people commit crime; that is to make money out of people's weaknesses. But there also are other reasons.

Malware viruses such as key loggers are able to obtain people's data and passwords by reproducing the input which users type on their keyboards; mainly for the purpose of obtaining private information such as passwords and other login details.

By doing so, criminals can potentially access many of the services we use, from our emails to our bank accounts, going through our online dating life. They can then try to empty our bank accounts using stolen credentials, or even use those details to purchase items online.

Furthermore, some of our more private information could be used as potential blackmail in order to extort some money from us.

Some other viruses such as adware are there to try to redirect our web searches onto specific advertisement pages, with the purpose of getting us to buy specific items, exposing us to many advert popups. This kind of virus will often insert itself into our user interface; often our web browsers.

When trying to access a page, we will often be redirected to an advert page, making our online web navigation very difficult by bombarding us with advertisement.

Other forms of malware include Trojan Horses, a form of harmful code which will hide inside people's computers undetected and can be used for a variety of purposes. Once again, Trojan horses are often used with criminal intent, mainly sabotaging existing system.

The purpose of this can vary from industrial misconduct (crippling the competition) but more often than not is mainly used by people whose ideologies go against their targeted companies. By crippling a whole companies' network infrastructure, they try to stop those companies from operating.

Some other viruses such as CryptoLocker are programed to simply destroy data, which is what this article is mainly interested in. The purpose of this sort of virus will be shown in the following paragraph.

CryptoLocker: the ransomware which can destroy your data

As the title says, CryptoLocker is a form of ransomware. What it does is pretty clever. It invades our computer and encrypts some of our most used files, making them impossible to access by their original user.

CryptoLocker will encrypt files which we really need and have spent a lot of time working on, from our text files to our game saves.

Once we try to open or use those files, they emerge as a different encrypted format, making it impossible for us to open those files, instead showing us corrupted an unusable files.

Once a user's computer is a victim of this sort of ransomware, they will be contacted by the perpetrators with a ransom demand; asking the user to pay for their data to get released back to them in a usable format.

Of course, there is no guarantee that the blackmailers will actually release the files after they have been paid, so it is pretty much a lose-lose situation for the user.

This kind of infection does not just occur to individuals but also to companies whose servers have been infected, making the original data impossible to recuperate as the infection takes place on a root level. As a result, the virus then gets spread to as many computers within the company as it can infect, resulting in many inaccessible files and a very high ransom demand.

What can be done about CryptoLocker?

CryptoLocker is a very difficult virus to get rid of and once caught, the likelihood of recuperating the original data is close to zero. This is unless the user has kept spare copies of their data in an unaffected separate drive. The idea is to keep spare copies of the original files before the infection takes place, as there is very little which can be done after the files are infected.

There are however instances where services such as Kroll Ontrack file recovery where able to recuperate and salvage some files from CryptoLocker infected hard drives. This can be seen in their blog here. It shows the case of a pharmaceutical company who got 46 of their hard drives affected by the virus because of one of their employees miss-handling their personal data and visiting unsafe websites.

In this case, the targeted company used a file system called the Netapp WAFL file system, which creates checkpoints of the data by saving different instances of those files overtime. This allowed Kroll Ontrack to recuperate older versions of the files which enabled them to access the original unencrypted copies of the files.

Since then, some tools have been made available on the internet which can help restore some of your files to a previously backed up version.

Regular file backup programs such as CrashPlan can help to ensure our files get regularly backed-up so that previous versions can be accessed. This is more of a preventive measure than a solution.

It is worth noting that software such as Malewarebytes can remove the CryptoLocker virus from infected computers, but unfortunately it does not recover the infected files themselves. So sadly, the matter of fact remains: if there are no existing previous unaffected copies of the files, then files affected by CryptoLocker will be difficult, if not impossible to recover.

Avoiding CryptoLocker?

As previously mentioned, the only true ways to avoid being a victim of the CryptoLocker ransomware is by using good prevention. Keeping spare copies of our files on a separate drive is a best practice all around, though of course it is not always allowed by certain workplaces. But at least when it comes down to individuals, the best advice is: **backup, then backup, then some more backup!**

Of course, viruses don't just get magically born, they often come from low security websites and websites which provide dubious content such as some file sharing services providing pirated movies and music downloads; and other content which is not safe for work.

Viruses mostly get caught by people so enforcing strict staff web browsing guidelines, as well as good staff training should limit those unfortunate instances.

Beyond prevention and upon realizing a computer is infected with ransomware, the best bet is to contact a data recovery company, as they know what they are doing and are some of the rare people in a position to be able to help recover some of the files.

Like with a lot of viruses, prevention is key. It is vital to use safe practice and also to use appropriate anti-virus software which can detect early instances of the virus before it spreads to the rest of the computer; if not the whole network of computers!

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/

The truth about Windows 10 spying on almost everything you do

You have probably heard the news by now: Microsoft has updated a controversial service agreement that lays out in scary detail how your personal data is being used and abused – at least, that's what the major tech blogs are saying. But the reality is, even if you read the 12,000 word service agreement, it's still confusing and vague at best.

Horacio Gutierrez, Deputy General Counsel of Microsoft's legal and corporate affairs, wrote about the company's commitment to transparency on the Microsoft blog in early June. This move, of course, was preceding the new privacy statement and service agreement that accompanied the release of Windows 10.

As he put it, "We are simplifying the services agreement and privacy statement because we believe that real transparency starts with straightforward terms and policies that people can clearly understand. As our services evolve, we recognize we must continue earning your trust."

How Windows 10 is spying on you

The reality is, we can't know what Microsoft is doing with your private data, but the release of the updated privacy policy and service agreement can give us some great insight. Yes, these long and tedious documents leave a lot of room for interpretation, but they also inspire something important: a discussion about how data harvesting and lack of digital privacy has become normalized.

Cortana: your personal assistant, or spy machine?

Cortana is your voice-activated personal assistant, much like Siri and Google Now. But in order for her to operate, Windows 10 collects your personal information to better serve you. This includes calendar events, contact information, alarm settings, what you view and purchase, your browsing history, emails and text messages… "and more".

An advertisers greatest dream

You may not have realized it, but each user on each Windows device will be issued a unique advertising ID that is tied to the email address they have on file. The idea is that you will be better served through ads, because according to Microsoft, "Advertising keeps many of the services you use free of charge".

Microsoft will share this profile (created from information aggregated from your personal files) with their partner ad networks – who in turn serve you ads on certain applications, like solitaire. If you

were concerned with ad networks collecting information from your browsing history, then be aware that Microsoft is taking it to the next level with Windows 10.

Data syncing with OneDrive

OneDrive is Microsoft's cloud storage system, and it comes with the Windows 10 territory. You might think it's great because there is no additional sign up or installment required and you can access it from any of your Microsoft devices. But this new convenience comes with a price.

Every time you are signed into your machine with your Microsoft account, your operating system immediately syncs your settings and other data to company's servers. This includes browser behavior and history, as well as mobile hotspot and Wi-Fi network passwords.

What are they doing with this information?

If you had the time to read through the long privacy policy and service agreement, you might get a vague understanding of what Microsoft will do with your data, but little more. Besides, we all know better than to take giant corporations for their word – they have their own interests to look after. The real questions end up being, what can Microsoft do with this information? And ultimately, what are they mostly likely to do with it?

Advertisers can "serve" you better!

People are getting used to free services online left and right, so these expectations dominate the tech marketplace right now. Windows 10 doesn't cost you any money, but it still comes at a price.

As Alec Meer of Rock Paper Shotgun points out, Microsoft is increasingly trying to compete with Google through software and applications. But this model requires that, "money comes from harvesting data and flogging it to advertisers and other organisations who want to know exactly what we're all up to online".

Comply with big brother

Microsoft doesn't beat around the bush when it comes to surveillance state issues:

Finally, we will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to: 1.comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies…

It's important to note that while this may seem horrifying to some, it's really not so different from any other privacy agreement. Just take a look at this snippet from Apple's privacy policy:

It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.

At the end of the day, there are few companies that are able to take a stance against big government agencies. The best you can hope for is providers who don't bury this in privacy agreements, but who are upfront and honest about their current operations as they relate to the surveillance state.

What could go wrong? Why should I care?

As an infamous activist once said, "Arguing that you don't care about privacy because you have nothing to hide is not different than saying you don't care about free speech because you have nothing to say."

But if that's not reason enough to get up in arms, there are a number of practical concerns to consider. First and foremost, you don't know which ad networks this data is going to, and you don't know what their policies for dealing with this very private information are.

What happens in the event of a hack? You might feel safe if your information is with a big company like Microsoft, which undoubtedly has major systems in place to protect your data, but do you really trust any of Microsoft's ad network customers? A hacker could trace these transactions and conduct a large-scale hack just by finding a single vulnerability in this line of data transfer.

You might say you have nothing to hide, and that the only person who does is clearly breaking the law. If that's truly the case, why don't you leave your bank account details in the comments below?

The real truth: Microsoft isn't the only bad guy

Shifting tides in modern culture have created two dangerous and commonly accepted thoughts on digital privacy, which could make you think that:

1. Privacy must be compromised for safety.
2. Privacy must be compromised for convenience.

While there are serious debates on the subject, it's important to stop and wonder who is ultimately responsible for these ideas, which create the basis for how many companies, institutions, and individuals make their decisions about privacy.

But the reality is, the Windows 10 privacy agreement isn't so much a revelation as a sign of the times. While it has understandably stirred up some controversy, it hasn't inspired a mass exodus from use of Microsoft software or products.

This is as it should be, because most of us know that it isn't different with the developers of other major operating systems and mobile operating systems…like Apple and Google.

Siri's telling everyone what you did last night

Sure, Apple and Google may have made a show of their commitment to user privacy, with smartphone encryption and very convincing, public battles with high-profile government agencies.

Apple has admitted Siri voice data is being sent to third parties

But you shouldn't let these PR stunts fool you. Even when these companies have the best intentions, there is still a bottom line at the end of the day, and that's money.

Don't believe us? Cortana isn't the only personal assistant who likes to abuse your privacy. Apple hands your voice recordings over to third parties for analysis, and you agreed to it in the privacy agreement. Whether it's a personal message to your sweetheart or your child asking Siri silly questions, Apple stores those messages for two years and essentially does with them what they want.

It might be tempting to switch over to Google Now for your voice commands, but that would come at the cost of both your privacy and sanity. Google Now has a feature called Now cards, which are recommendations for products, services, and information based on your messages and recent searches.

Even if you don't rely on Google Now too much for recommendations, Google already knows so much about you because at some point you have probably used their products or services.

And if you use Gmail, you'll note that Google has been serving ads through Gmail for some time now – and if you haven't noticed any, just check under your Gmail's "Promotions" tab.

They get information straight out of your private emails to help their ad network partners target you. It's right there in their privacy agreement.

Microsoft even attacked Gmail over these privacy violations and launched a "You got Scroogled" marketing campaign.

What you can do to protect your privacy

The reality is, short of becoming a Linux user or developing your own operating system, there is little you can do to keep your information entirely private.

Even recent Windows 7 and 8 updates come with their own host of privacy issues, so don't think you're out of the woods just because you haven't made the move to 10.

But there are several steps you can take to maximize your privacy while using Windows 10, and we encourage you to explore these options – whatever agency you can take over your privacy is better than none.

Windows 10 setting options to look into

If you have yet to install Windows 10 be sure to decline the Express Settings, which enables all of the privacy compromising features. Look through the different setting options and disable anything that makes you uncomfortable.

If you already enabled the Express Settings when you downloaded Windows 10, go to the start menu and select Settings.

From there you'll find that most of these invasive features are listed under Privacy. There are many options to go through, and we encourage you to look carefully at each one.

There are several big ones we think you may want to consider disabling:

Cortana

You may not be comfortable with Cortana collecting so much personal information about you, and if that's the case, you should disable the Getting to know you option under Speech, inking, & typing (this is located in the Privacy box).

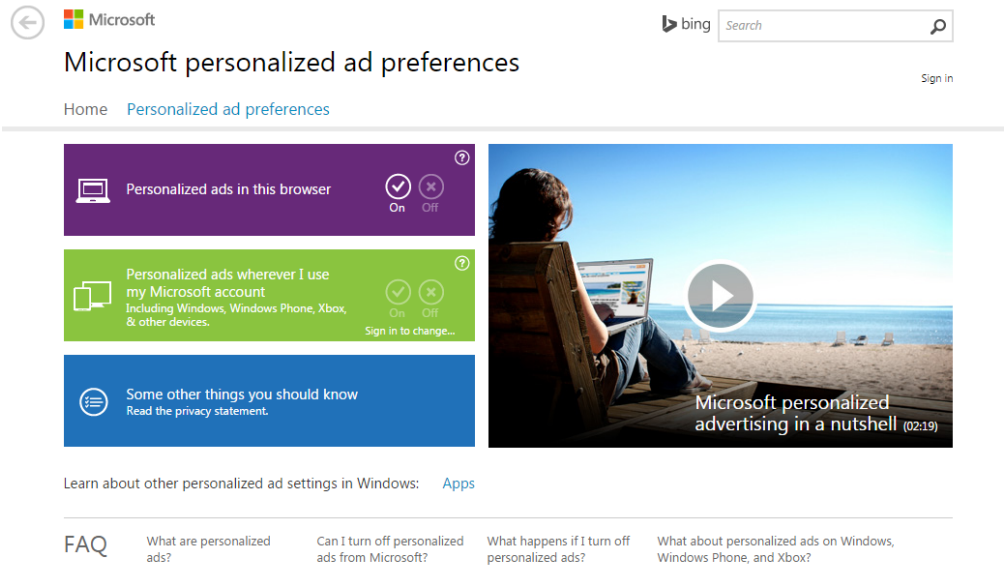
Additionally, you can click on the gear icon where you can access the Cortana settings, where you can enable or disable her (as well as manage information kept about you in the cloud).

Advertising ID

If you are concerned about the data harvesting for advertisement purposes, we do recommend you disable setting, "let apps use your advertising ID for experiences across apps".

This is located underneath the General tab in the Privacy box.

Unfortunately, just moving the toggle isn't enough to keep ad networks from reaching your personal data. You will also have to go to this Microsoft site and disable personalized ads several times over.



Microsoft allows you to personalize your ad settings

Location

You may be used to location services, and they sure are handy when you're trying to get from point A to B. But Microsoft's new privacy agreement suggests they are sharing this location information (and your location history) with "trusted" third parties. If that makes you uncomfortable, it may be best to disable this. The Location tab is located directly beneath the General tab.

Wi-Fi Sense

Wi-Fi Sense could be either very practical, or very invasive, depending on how you look at it. The new feature allows you to automatically share your Wi-Fi password with your Outlook, Skype, and Facebook contacts, which saves a lot of hassle when friends come over and need your password.

Windows 10 Wi-Fi Sense: do you need it?

On the other hand, this may not be wise for those with broad social networks, because this option does not allow you to selectively pick which contacts to share it with. This option should be enabled or disabled on a case by case basis – it's located in Network & Internet instead of Privacy.

Use a local account

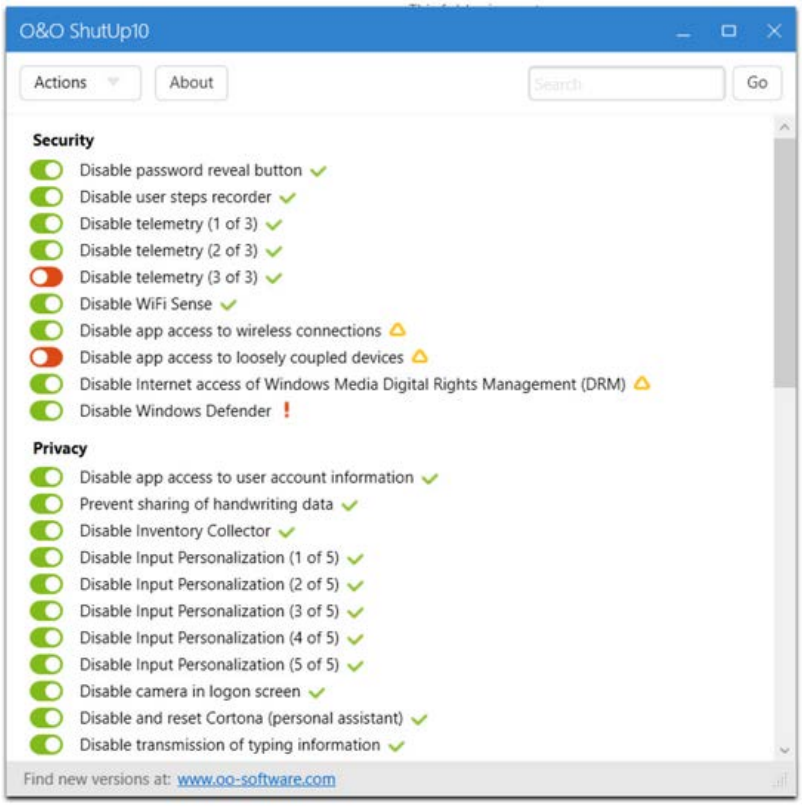
If you're not concerned with convenience and want maximum privacy, you should consider a using a local account instead of your Microsoft account. You will lose out on a number of features, particularly synchronization across your different devices. But if that doesn't bother you, locate Accounts under Settings, then click Your account. You should see the option to "Sign in with a local account instead" just above where your picture should be.

Try O&O ShutUp 10

O&O ShutUp10

If you'd like to simplify this process, consider using O&O Software's free privacy tool, ShutUp 10. This tool simplifies the privacy process by giving you a single interface to deal with all of the myriad of settings you'd like to enable or disable on Windows 10. You can also simply apply all of their recommended settings.

O&O ShutUp10 is entirely free and does not have to be installed. Moreover, it will not install or download potentially unwanted or unnecessary software (PUPs), like so many other programs do these days!



O&O ShutUp10 allows you to easily disable Windows 10 settings

Educate yourself about privacy options that feel right for you

At the end of the day, you might be tempted to throw up your hands and give up perusing privacy at all. You might not see the point, since disabling certain settings doesn't really guarantee that you are not being spied on, or that your personal data isn't being sold or distributed.

You might feel that you might as well have the conveniences of certain tools then, or would prefer more relevant advertising.

But if we all collectively begin to educate ourselves about our privacy options and pursue them, we have a better chance of creating a culture that is concerned with cyber safety and privacy, instead of one that just thinks it's a cost needed for a better world.

Have a nice (privacy-conscious) day!

About the Author

Christian Mairoll Contributor, Emsisoft

Christian is founder and CEO of the Austrian anti-malware company Emsisoft.

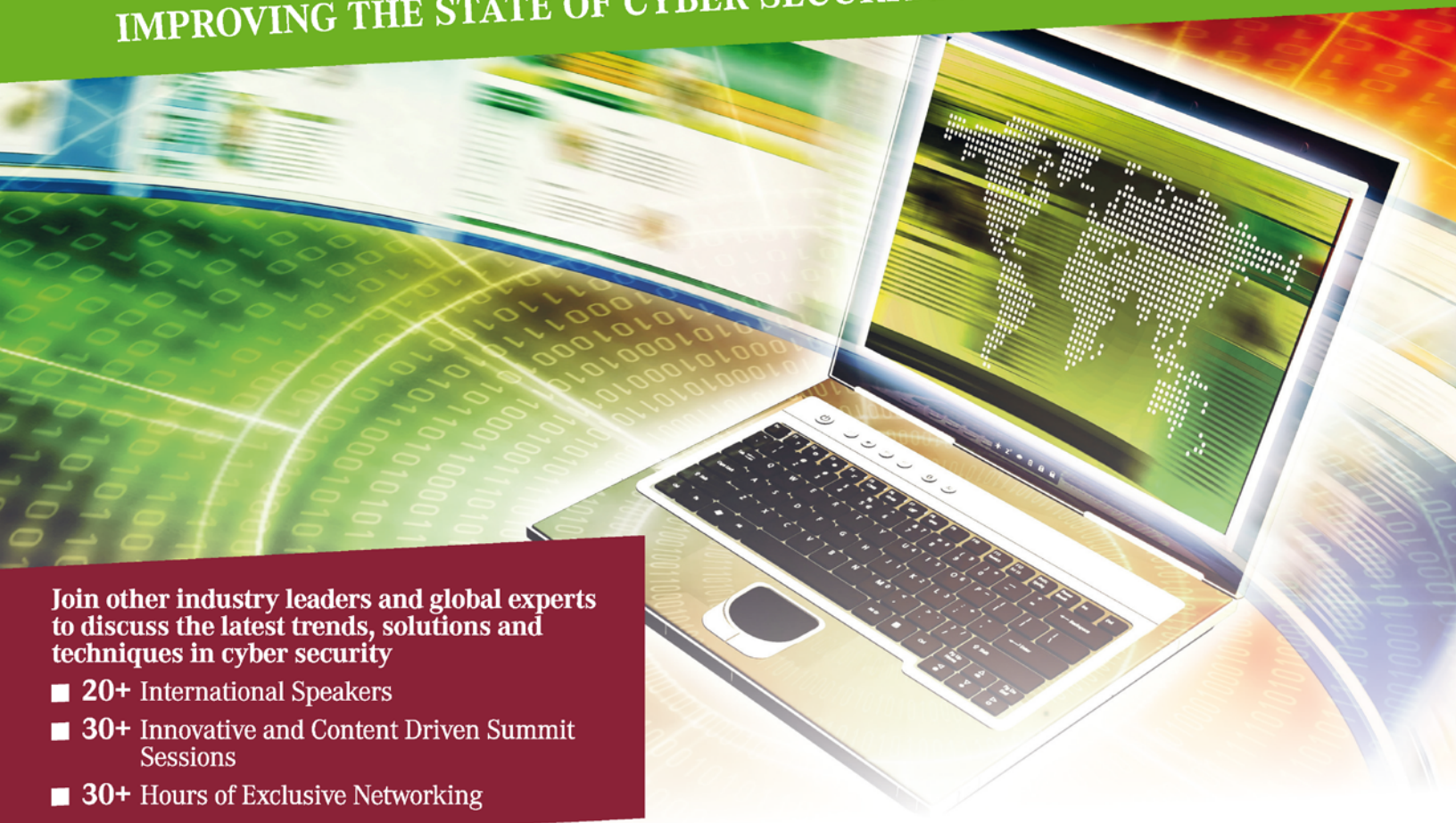
For CDM, his aim is to educate our readers with essential security knowledge, especially in understanding and stopping new and innovative malware.

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 CONFERENCE
MANAGEMENTCIRCLE®

www.cybersecurity-leaders.com

How to Find a Good Website Security Scanner

Hackers have continued infiltrating the internet and they are always trying to hack websites and leak important data that may harm any organization's reputation. Website security scanners play a huge role in testing and identifying any security vulnerabilities your site may be exposed to.

Security scanners do not access the source code; they only perform functional testing and try to determine the vulnerabilities. It is important to take a few factors into consideration before making any purchasing decision. Here are some tips that will help you choose the right website security scanner that fits your needs.

Requirements

As a website owner, you are likely to have a list of requirements in mind. The requirements may include automation of tasks, lowering your web application security costs and increasing your coverage. Automated website security scanners are highly recommended as they help to save time as well as identify all technical web vulnerabilities.

Ease of use

A good website security scanner should be easy to use as the subject of web vulnerability scanning is already broad and difficult. You should spend most of your time fixing the threats detected instead of figuring out how the scanner operates.

Security tests it can carry out

Most website security scanners are able to identify common web vulnerabilities present. However, the scanner you choose should also be able to identify vulnerabilities that are less widespread.

Variations of the vulnerabilities

In addition to being able to identify a variety of vulnerabilities, a web vulnerability scanner should also check and report on the variations of the vulnerabilities found. An example would be the Cross Site Scripting, where a web developer may fix the simple version of the vulnerability, but might fail to tackle the vulnerability when the Cross Site Scripting payload is encoded.

Ability to cover content management systems

A lot of organizations use content management systems like Joomla, WordPress and Drupal to create content on the site regularly. All this content management systems are prone to their own set of vulnerabilities. The website security scanner that you use should be able to check these for configuration errors and possible vulnerabilities in the systems.

Ability to cover web technologies

Most web applications use JavaScript, HTML5, Google Web Toolkit and Single Page applications. A vulnerability scan crawls the web application to identify the pages, forms and elements that make up a given web application. When choosing a web security scanner, it is important to go for a scanner that is able to understand the intricacies of web technologies used in a variety of web applications.

The scanner should also be frequently updated to ensure that it is able to crawl latest technologies in future.

Ability to scan mobile friendly website applications

Several web apps have a friendly mobile version which is automatically loaded on tablets and smartphones. Although they often provide the same functionality as the main website, they are also just as vulnerable as the main site. Your website security scanner should be able to also scan the mobile friendly site to ensure that it's not exposed to web vulnerabilities as well.

Availability of manual testing tools

An efficient web security scanner should provide manual testing tools to verify some of the vulnerabilities detected after an automated scan.

Grey Box testing

Several web vulnerability scanners provide black box testing since they are able to scan your website without accessing the source code on the web server. A good web scanner should also provide grey box testing which enhances the scan results by ensuring complete coverage of web applications. It can also detect more vulnerabilities compared to black box testing.

Grey box testing also decreases false positives by providing supplementary validation and information on the vulnerabilities detected.

While several web security scanners are authentic, you need to be careful on scanners that make empty claims. Scanners claiming 0 false positives should be avoided at all costs since they may not be showing vulnerabilities or they may fail to show that more testing is needed.

About the Author

Lee Ying has over 10 years experience in the tech and security industry. He currently writes for various websites, if you would like to contact him you can find him on LinkedIn: https://www.linkedin.com/pub/lee-ying/9a/18b/238. Follow me on Twitter @LeeYing101

It's Only A Game!

By Margie Sloan

Violent video games offer a cornucopia of cyber security issues for players. Games that provide hours of entertainment and competition to millions of adolescents, teens, and adults all over the world, also extend a gracious invitation to those with an unholy agenda. However, gamers rarely concern themselves with cyber threats.

Photo by Jeff Watts/American University

Scott Talan States 'Isis is using Madison Avenue techniques' to recruit gamers.

Going on line and getting a game on is paramount to the gamer intent on mastering a skill at games that depict torture, abusive sex and killing. The graphic brutality and glorification of hate driven combat fits right in with the ISIS call to jihad. The gamers at ISIS favor Rockstar Games Grand Theft Auto V (GTA5) so much so that they have their own version of it available for all to see on the internet. The gamers at ISIS don't mince words on their version of GTA5. "Your games. We do the same action on the battlefield." ISIS also modified Bohemia Interactive's ARMA 111 so players could become virtual mujahideen. Al Qaeda used Blizzard Entertainment's World of Warcraft for their pep rally.

Winn Schwartau warned in 1991 of an electronic Pearl Harbor

These modern day cyber toys are now cyber tools for propaganda. John Carlin, United States Assistant Attorney General, National Security Division said that ISIS is trying to convince young people to go slaughter civilians in a vicious war. Scott Talan, Assistant Professor of Public and Strategic Communication at American University said that the threat of ISIS using games for recruitment is real. "All it takes is one successful terrorist, but it's a confluence of forces that exist prior to using any tool like a game to get anybody to join them." Talan pointed out that ISIS is using Madison Avenue techniques. "It's ironic that while espousing anti-western sentiments, they use


Gloria DeGaetano and Lt. Col. Dave Grossman
"Stop Teaching Our Kids to Kill"

western made products in their media campaign."

Winn Schwartau, Founder and CEO of the Security Awareness Company testified before the United States House of Representatives on June 27, 1991 and warned about the weaponization of the internet. "I was asked by a Congressman, 'Mr. Schwartau, do you really believe that the bad guys are ever going to use the internet for something evil?' What scares me is that what was predicted twenty years ago is now a part of our daily lives. There has been a great abuse of technology that we didn't see coming and we ignored a huge amount of it. This scares the IT out of me."

Schwartau also testified that he was less worried about hackers and more worried about organized and funded organizations with reasons to penetrate. Today, millions of gamers in every corner of the world are in virtual boot camp, preparing for heinous acts of war. The best selling first person shooter games leave nothing to the imagination with depraved actions that are unimaginable to anyone valuing human life.

First person shooter gaming offers an escape from boredom but can lead to danger. Gloria DeGaetano, CEO, Parent Coach International and Lt. Col. Dave Grossman, United States Army Retired and Director of the Killology Research Group wrote in their book, *Stop Teaching Our Kids to Kill*, "As graphic as the violence is on TV and in movies, it can't quite compete with a medium where you, not an actor can control the action."

Kim Komando
Syndicated Radio Talk Show Host

The targets that terrorists and sex offenders go after are the addicted young gamers who are disassociated and long for a tribe of their own. They play games with a focused and often manic fervor. These are the potential lone wolves who can spring into action when the call is heard, catapulting themselves to heroism by taking their skills to the streets. Iowa State University Professor Douglas Gentile's study of gaming shows that one out of eleven will get addicted. He says, "Violence is a complicated adult issue. Kids aren't emotionally or cognitively prepared to think about the ramifications."

Schwartau raised the addiction issue in 1995. "I asked Bill Gates in a public forum, 'What do you think about the addictive aspects of the internet and computers and how we will have to handle this on a social basis, much like gaming, as in the book on addiction, *Game Over*?' Gates paused, looked at me with superiority and said, 'It'll never happen.' I tried to discuss it with him in more detail at a press conference we shared, and his handlers kept me away from him."

Andrew Doan M.D. P.H.D.
Head of Addiction and Resilience Research in the Department of Mental Health, and Gamer

Gaming is today, a dangerous digital drug as addictive as heroin, according to Dr. Andrew Doan, MD, PhD, Head of Addiction and Resilience Research in the Department of Mental Health, United States Naval Medical Center San Diego. Doan was hooked on games, quit and then took an objective look at what happens to the mind and body when games produce a thrilling high and become an obsession. In a recent address at the Great Lakes Naval Station, Dr. Doan told his audience that gaming addicts crave the euphoria they get from their computer screen as endorphins are released into the bloodstream and dopamine into the brain. This is just what the games are intended to do. Doan pointed out that game companies study gamers

and track spikes in heart rate and blood pressure, and also measure the PH balance in sweat. The buzz word for this research is "neurogaming. "The nerve biologists the companies hire place electrodes on gamers and turn up the action on the game so that the blood pressure goes to at least 180," said Doan. The data from these physiological signals are then incorporated into the game to make it more of an exhilarating experience. If the desired intensity isn't met, the writers go back and adjust the content to give the player the perfect storm. The anonymous gamers who are up to no good bank on this and seek out the addicted gamer who is always available.

"It's easy for really bad guys to get a game, become the preferred game buddy and grab an unsuspecting player," said Doan "When you get to a higher level of competition in gaming, it's the thrill of playing and possibly winning that matters. Gamers are not aware of the location of the opponent or their true identity, and that player could be anywhere there is an internet connection, including hot spots for human trafficking, ISIS and al Qaeda."

"Don't trust game companies, social media sites, online retailers or any other company to protect your kids."

Sadly, this is just what happed in New York in 2011 and in England in 2014. Richard Kretovic in New York engaged with a 12 year old boy on Xbox Live for three months, buddied up to him and invited him to his house where he sexually abused him. Shortly afterwards, New York State Attorney General Eric Schneiderman initiated Operation Game Over in New York where gaming companies agreed to shut down the accounts of over 3,500 registered sex offenders in New York State. Schneiderman said, "We have to be vigilant in this area because on line gaming is not just a digital playground. It has the potential to be a 21st century crime scene." Ahmed Muthana in England lives with the fact that his two sons, Nasser and Aseel are no longer a part of his life. He is convinced that they were recruited to fight with ISIS after playing Call of Duty: Ghosts.

Syndicated talk radio host, columnist and computer expert, Kim Komando said that many parents don't recognize the dangers as they didn't grow up with the same technology. "They need to understand that letting your kids talk with a stranger online is just as dangerous as it would be at your local park. The future is digital and online. We have to train our kids in the online world like we do in the offline world."

Opal Singleton, CEO of Million Kids and Training and Outreach Coordinator for the Riverside County (CA) Anti-Human Trafficking Task Force calls violent gaming a grooming incubator used by cyber criminals to ripen their prey. She said parents are not aware of the impact the games can have on young minds. "When I ask kids if they feel bad after killing a character in a game, they tell me no… that it's what they have to do to win. Young gamers live in a fantasy world and are being trained to shoot cops and have sex with a prostitute and then kill her so that they can get their bitcoin money back," said Singleton. "We have a generation of kids who have never not known the internet. Online gaming allows access, grooming, recruitment and exploitation by anonymous strangers using clever handles."

Opal Singleton
CEO of Million Kids
"Look behind the mask and hidden identity of the avatar and see the intentions."

Singleton works with educators, law enforcement and parents, both domestically and internationally. She finds that, "Kids have enormous peer pressure to be game winners, constantly updating their scorecards and revealing personal facts in the chat rooms. Parents need to know that nearly a million pedophiles and pimps have easy access to their child's thinking on morality, spirituality and sexuality."

The financial bubble of gaming is growing exponentially. Many Hollywood script writers now write for the gaming industry as the money is solid. Sales of GTA5 made a billion dollars in three days. The marketing hype had millions of gamers salivating for the newest and goriest in the series. ISIS was pleased and no doubt agree with DeGaetano and

Grossman who say that young gamers who "practice murder, torture and brutality day after day, can come to want, expect and seek murder, torture brutality and quite possibly then choose to act them out."

GTA5 has been under fire for its virtual abuse of women, another thing that their creators have in common with ISIS ideology. GTA5 offers players the first person experience of torturing, raping, and killing a woman, and then resurrecting or re-spawning her to do it again. When asked by Bloomberg News about this kind of violence in the game, Strauss Zelnick, the CEO of Take-Two Interactive, the parent company of Rockstar Games said that it is art and that he embraces that art. Zelnick also said that he doesn't play GTA5 or any other games and that his company provides a great experience. Great for whom?

Great for arms manufacturers Hawk & Little, Shrewsbury and Vom Feuer who see their products in the game, and certainly great for retailers and those who own stock in Take-Two Interactive, a public company. Maybe not so great an experience for the young gamers who develop unhealthy aggression, depression, isolation and addiction from hours of play. DeGaetano said, "Corporations feed off kids' vulnerabilities to images of sex and violence. For many, the bottom line isn't 'What's best for our most vulnerable citizens?' but rather, "How can we turn their vulnerabilities into greater profits?" Komando warns, "Don't trust game companies, social media sites, online retailers or any other company to protect your kids. Their first goal is making money."

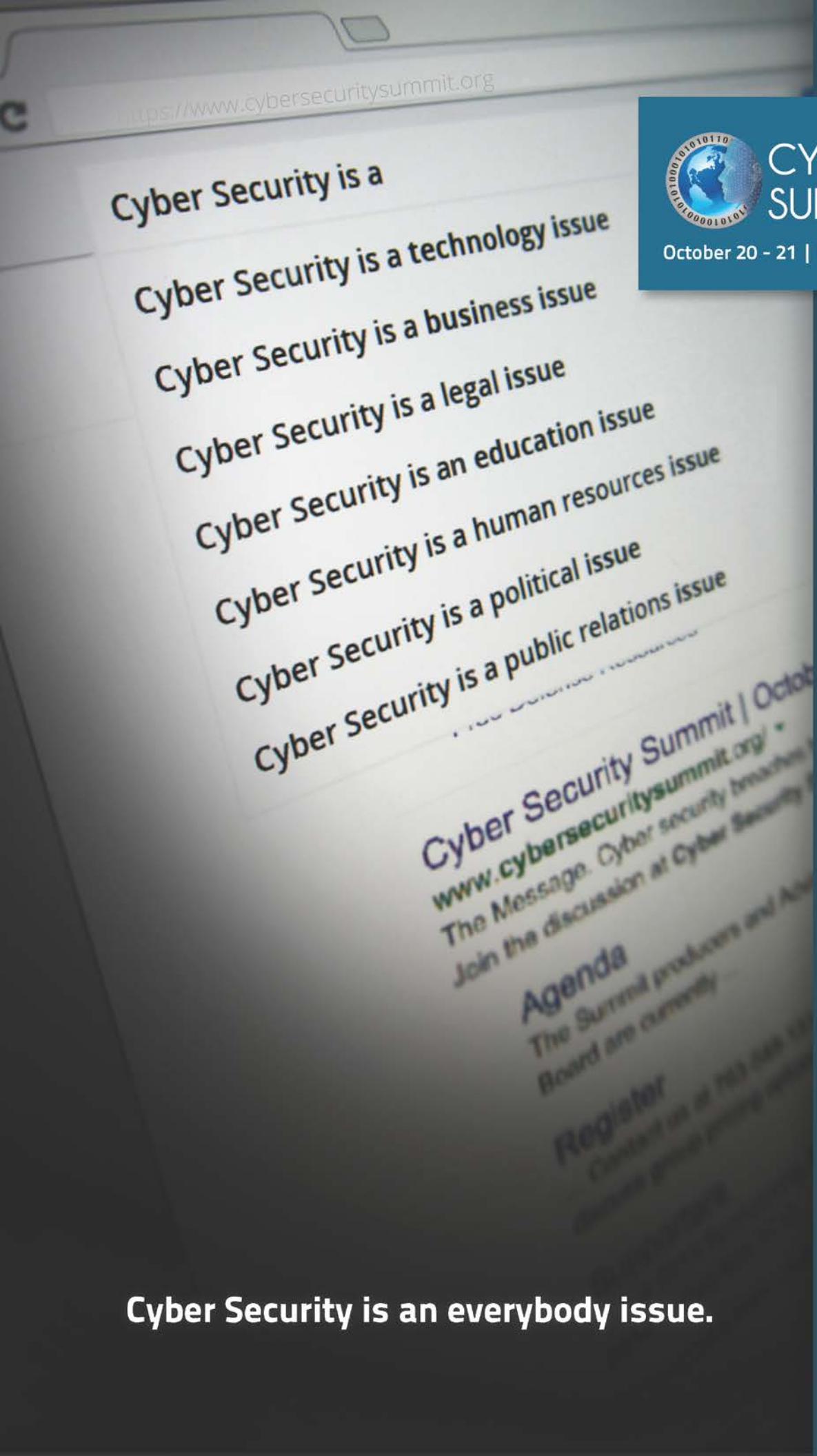
The great majority of gamers won't be confused as to what is real and what isn't and won't develop an addiction. Dr. Doan asks if we can take the chance and ignore the percentage that does get addicted and consumed with the violence. The chilling commonality shared by Eric Harris, Dylan Klebold, Seung-Hui Cho, Jared Lee Loughner, Anders Breivik, Adam Lanza, James Holmes and Aaron Alexis are violent video games. These avid gamers played to win and gave us their best shots at Columbine High School in 1999 with 15 dead, at Virginia Tech in 2007 with 33 dead, at Tucson, Arizona in 2011 with 6 dead, at the Norway Massacre in 2011 with 77 dead, at Sandy Hook Elementary School in 2012 with 28 dead, in Aurora, Colorado in 2012 with 12 dead and in the Washington Navy Yard in 2013 with 12 dead. Breivik told the court in Norway that he trained for his killing spree by watching Call of Duty: Modern Warfare.

The controversy over violent video games is nothing new. The United States Supreme Court protects them. There are privacy issues as gamers are anonymous to other gamers but the game companies know who plays their games. There's gold in the games, both figuratively and literally. The gaming industry pulls in billions each year. Major League Gaming rewards the winning teams playing Dota 2 and Call of Duty: Advanced Warfare with $500,000 in prize money. There are warnings available. The Entertainment Software Ratings Board gives detailed descriptions of game content and urges customers, especially parents to read them before purchase. The United States Military uses graphic games to help train soldiers as the games are close to the real thing. Celebrities Snoop Dog, Dave Chappelle, Mila Kunis and Ice-T are players. Hilary Clinton is against the violent games and New Jersey Governor Chris Christie doesn't allow them in his house.

What's new is that terrorists and child molesters have discovered a way to influence vulnerable players who might want to step up their game. Bombs truly are a blast and the knives used for beheading by ISIS killers are anything but virtual. They are real, horrific and serrated for maximum pain for their victims who are real people with families and friends. The monsters who target children are playing with the minds and emotions of their opponents. The fun of the game is over when the child is raped or killed or sold into human trafficking.

F.B.I. Director James Comey told his audience in Aspen last July that ISIS scares him more than al Qaeda and that he is awake at night worrying about an ISIS attack on American soil. Winn Schwartau in 1991 warned Congress of "an electronic Pearl Harbor." Opal Singleton said that over a million kids around the world are compromised each year on violent games. Dave Grossman said that denial of the problem is our enemy. Dr. Doan, a gamer, a surgeon and a neuroscientist said that the contagion of playing violent video games is just the tip of the iceberg. *Anyone remember the Titanic?*

Email: argiema@yahoo.com



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.

Cyber Security is an everybody issue.

www.CyberSecuritySummit.org

TVSPY - Threat Actor Group Reappears with Teamviewer Malware Package

By, Loucif Kharouni, Sr Threat Researcher at Damballa Inc.

What's TVSPY?

TVSPY is a malware that takes advantage of a vulnerability in Teamviewer software version 6, a legitimate tool used for remote PC administration. The malware is also known as TVRAT, SpY-Agent or teamspy.

While the current version of Teamviewer fixed this vulnerability, TVSPY relies on bundling Teamviewer v6 in a package with a copy of the malware. It works independently of any existing Teamviewer installation.

TVSPY: APT or Crimeware?

Eset and Group-IB discussed this malware as crimeware back in 2011 at CARO, while Kaspersky mentions it in one of their APT reports from 2013, with a detailed description of its routine. There seems to be an increase in the prevalence of these malware variants recently.

The number of unique variants we have already seen in 2015 is 4.4x the number seen in 2012, and 2.2x that seen in all of 2014. There are some instances of Dridex installing this malware as well. This malware has been relatively quiet for more than two years so the nearly three-fold increase in activity is concerning.

Year	Unique samples
2012	5
2013	8
2014	10
2015	22

More recently, a targeted email campaign included a malicious Excel file with a macro would download this malware. The email was impersonating the All-Russian Research and Design Institute of Nuclear and Energy Engineering.

The analysis of the Command and Control server for this latest variant appears to be owned by professional criminals.

```
001A39FC  001A39FC  0  er1=http://canterus.com/getinfo.php
001A3A21  001A3A21  0  nextsrv=120
001A3A2E  001A3A2E  0  dwl=http://canterus.com/files
001A3A4D  001A3A4D  0  dwlext=_
001A3A57  001A3A57  0  useragent=Mozilla/5.0 (Windows NT 5.1)
001A3A7F  001A3A7F  0  interval=60
001A3A8C  001A3A8C  0  password=
001A3AA0  001A3AA0  0  arun_type=2
001A3AAD  001A3AAD  0  arun_reg=1
001A3AB9  001A3AB9  0  arun_path=
001A3AC5  001A3AC5  0  arun_keyname=
001A3AD4  001A3AD4  0  arun_fldname=Windows Update Manager
001A3AF9  001A3AF9  0  arun_flddescr=Windows Update System Service
001A3B26  001A3B26  0  arun_flddll=shell32.dll
001A3B3F  001A3B3F  0  arun_fldindex=46
001A3B51  001A3B51  0  runexe=
001A3B5A  001A3B5A  0  runbro=0
001A3B64  001A3B64  0  runalways=1
001A3B71  001A3B71  0  runsilent=1
001A3B7E  001A3B7E  0  vpndel=1
001A3B88  001A3B88  0  volid=1172548
```

Image 1. TVSPY config file

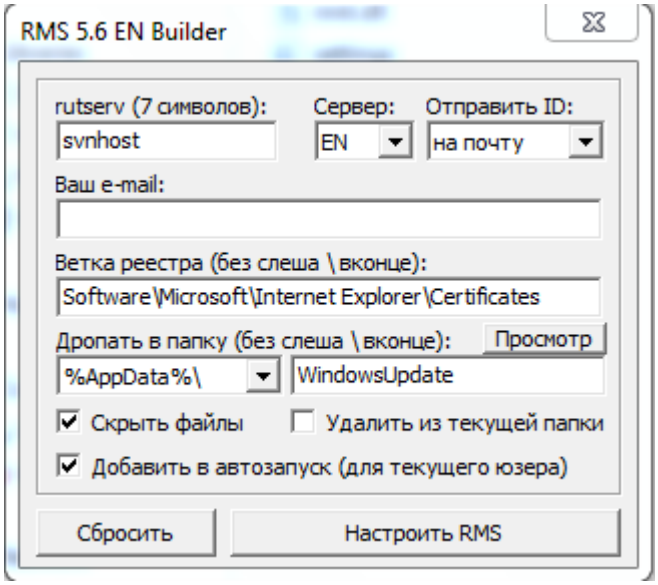


Image 2. RMS 5.6 builder

Image 3. TVSPY CnC panel

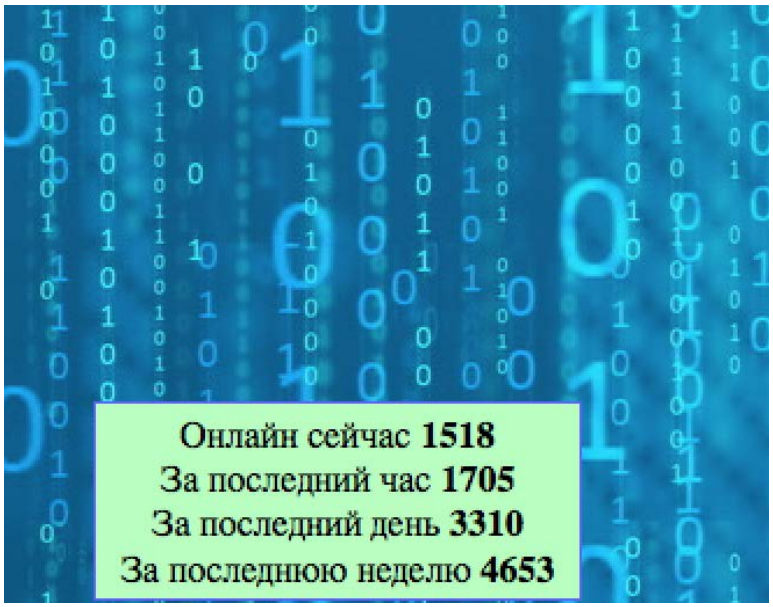


Image 4. TVSPY CnC Panel stats

Who sells TVSPY?

Scalpel started to sell this malware on criminal forums last June 2014 for $400. He took over the sale for Mr.Burns. The original malware was created by Mr.Burns, he created something similar called RMS. Mr.Burns found a way to take advantage of Teamviewer v6 using a DLL to hijack the session. Teamviewer v6 was released in 2010. We were able to obtain a public version of RMS 5.6 that looks very much like the TVSPY builder. Mr.Burns recently deleted his youtube channel where he had 2 videos showing how RMS and TVSPY work.

Scalpel information:

Handles:
scalpel
brutalisk
overd0s3r

Emails:
bio@insorg-mail.info
scalpel@insorg-mail.info
missis.ljasan@yandex.ru

Jabber:
scalpel@jabb3r.net
sl@adium.in
sl@exploit.im

Mr.Burns information:

Name used in Youtube/Google+:
Иван Иванов - Ivan Ivanov

https://plus.google.com/104153253633611754625/about

Handles:
Mr.Burns

Emails:
sonofabitch@ua.fm
mrburns@nm.ru

Jabber:
mrburns@jabber.se

Skype:
mr.monty.burns

ICQ:
610047

A video demo of Spy-Agent was posted on YouTube, but has since been deleted:
https://www.youtube.com/watch?v=QWRfGxBDwEQ

pic4a information:

Jabber:
pic4a@exploit.im
pic4a@fuckav.in

Conclusion

This particular threat is very dangerous as the attacker will have total control over the affected machine. We see that it can be used during a regular infection campaign or by some APT actors for specific attacks against particular targets.

RMS/TVSPY continues to be developed, with a new version being posted by the developer/reseller on a regular basis.

In fact, the legitimate RMS version developed by TektonIT and the version posted in criminal forums appear to be identical.

TVSPY seems to be merely a modification of RMS to utilize TeamViewer infrastructure and a command and control interface manageable through the web.

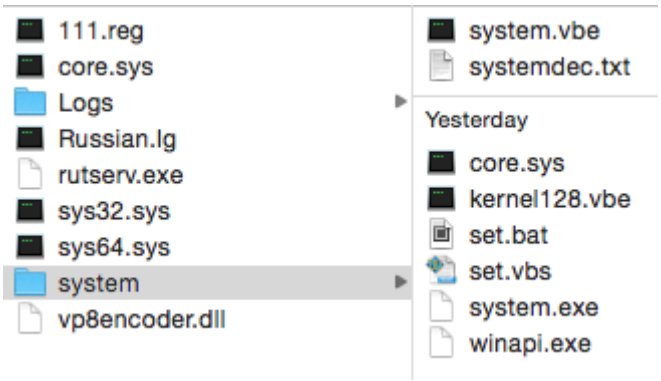
Damballa detects TVSPY as BlueSpiderCrashers.

Loucif Kharouni
Senior Threat Researcher

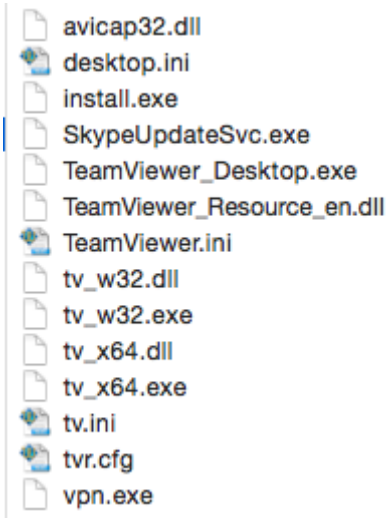
Willis McDonald
Senior Threat Researcher

Indicators of compromise:

- Under C:\kernel (folder kernel has hidden attribute):



- Under C:\Users\[UserName]\AppData\Roaming (all files use hidden attribute):



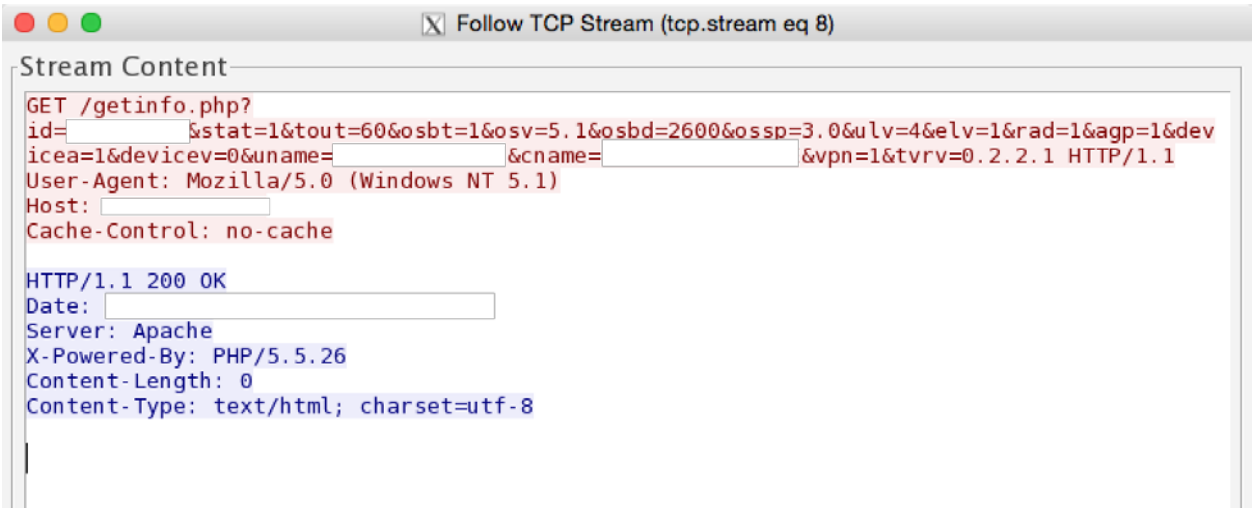


Image 5. Infected machine beacons to CnC

Here is a text version of the GET request made by the malware:

/getinfo.php?id=[0-9]{9}&stat=1&tout=60&osbt=1&osv=5.1&osbd=2600&ossp=3.0&ulv=4&elv=1&rad=1&agp=1&devicea=1&devicev=0&uname=[username]&cname=[computer_name]&vpn=1&tvrv=0.2.2.1

Variables	Definition
id=[0-9]{9}	id is a random 9 digits number associated to the infected machine
stat=1	

tout=60	
osbt=1	
osv=5.1	Windows version
osbd=2600	Windows build version
ossp=3.0	Windows Service Pack version
ulv=4	
elv=1	
rad=1	
agp=1	
devicea=1	
devicev=0	
uname=[username]	username
cname=[computer_name]	computer name
vpn=1	vpn on
tvrv=0.2.2.1	tvspy version

The last variable is particularly interesting as this is the first time we have seen it. Other samples we analyzed have not displayed this variable.

Command and control servers:

5.45.70.137/stats/getinfo.php
78.47.135.84/contacts/getinfo.php
91.121.44.159/tvddj39/gerinfo.php
91.215.155.46/tv/getinfo.php
91.215.155.48/tv/getinfo.php
92.53.96.101/getinfo.php
109.234.35.77/btrtrxirmi/getinfo.php
162.211.230.170/tv/getinfo.php
178.63.249.40/awstat/getinfo.php
194.63.142.171/tv/getinfo.php
206.su/admin42/getinfo.php
ac.myjino.ru/getinfo.php
aflnatour.ru/admin/getinfo.php
aflnatour.ruadmin/getinfo.php
bestkassa.com/tb/getinfo.php
blackvfl.com/tv0/getinfo.php
bo1324522.com/tv/getinfo.php
cdn-rskp.com/cdn/getinfo.php

cofewariiroirm.ru/1/getinfo.php
darlingday.ru/getinfo.php
doomns.mooo.com/getinfo.php
f1rst.name/tv/getinfo.php
filidaro.com/rvbtdsf/getinfo.php
jmai1.com/tv/getinfo.php
mmm-svoboda2012.ru/getinfo.php
nynewsguardianinternet.com/NotebookFront/getinfo.php
statisticsystic.com/telekinect/getinfo.php
tim-t.ru/getinfo.php
tvincoming.com/adm/getinfo.php
util4u.com/ctrl/getinfo.php
wowcofes.ru/getinfo.php

Hashes:

a55149b4164659d5c0e1cd2daef9a702
21670682a47021cc4be53ea832df7dbd
efa5c157946125734184a1cb62c6a0e1
f84928ea5b4752b9cc2a7ae2155d6fd5
688be0a5684dbe633ea86d3640e33d47
070859ed01990f003b78d9820e77d72e
9146902c590c98b8b2c4bb7d323623cd
c3de5426a4fec6e97acd1f693081615e
8852fb707e1a5c5d505b6a026e8ddab5
718633f40da55c76f0c6c7c81824799f
b36a11b189242e071e8c8e564aab56e2
2afa10d90a4899f9215f77b1db9230e3
99bdcab182678da0dcf52aa4a0795b05
d88e492a0c91441bc4385e0dfe69caf2
09e20b095e0aa1d8aa2f9c16ff76b1e9
407cd02af6ea3a7b2d4246ba8f89b076
71d1cf7dc21dfa5fa0a615cfa06dc297
255e3db5aa603384d2ca4594b18dc609
fd90061743e0f33ae5135cb2fbf7057e
0c368c121f13928d9699fbc93eead367
4414e69f4b895551f5a90abb59ff2330
30ebfdc2a2e90ccd0649ccdf853f1e9d
bc8eb8677390f90de921592c86f17040
3a8455584bda5951b8c0a05deed87b4f
eb88459f2d532fa3fcc081e2e6a1d549
008cc983f88b87f8b804988ac4c8d532
7a5972a7038f224ff97e02c13082e418
33d079af33b3689a9d6a9517b39c8d7b
5190aa75867dde7ca172c2c30d19dcf3

4a9fdd47041252608801d16b4ac11e12
b4dc51648fa10c349453d80c8cfabed2
13467f0886de6d0c6716ac0a4eeb2f59
c5c05c0f4b9e3b6ac2ad51dc15ef8f43
f7a4602db94cd67e9c03d918eaef91a2
8b0d8f1d06aea9bc5c7477c9c8284713
4c177ad2a07a304318d09fc4ef389a09
1a141a76d12f7a310ade141133c0a37c
a5aff9aa5b2e45a0f9fea080f8f15971
1a9b23d9e18c5d19e86fc5a89012a0ef
8230f1f93245528c1faa82d945c25332
18faa7856fda324ed06261368ab72829
b7ab83f84103130e46e95de0df8d85a4
740d9cd8ea165302aa3cd7e6f198ea4c
9079fc3edc31956ab63bbb23673e6c7c
1fe21a120f524bb914b210284e1caf05
36f2049cc1a5db224fcd6541d630677f
58f1852af6a270d385f270d60d00a0a5

Host and hashes:

Host	Hash
util4u.com	070859ed01990f003b78d9820e77d72e
aflnatour.ru	9146902c590c98b8b2c4bb7d323623cd
aflnatour.ruadmin	9146902c590c98b8b2c4bb7d323623cd
tim-t.ru	c3de5426a4fec6e97acd1f693081615e
aflnatour.ru	8852fb707e1a5c5d505b6a026e8ddab5
aflnatour.ruadmin	8852fb707e1a5c5d505b6a026e8ddab5
ac.myjino.ru	718633f40da55c76f0c6c7c81824799f
util4u.com	b36a11b189242e071e8c8e564aab56e2
mmm-svoboda2012.ru	2afa10d90a4899f9215f77b1db9230e3
tim-t.ru	99bdcab182678da0dcf52aa4a0795b05
mmm-svoboda2012.ru	d88e492a0c91441bc4385e0dfe69caf2
darlingday.ru	09e20b095e0aa1d8aa2f9c16ff76b1e9
util4u.com	407cd02af6ea3a7b2d4246ba8f89b076
mmm-svoboda2012.ru	71d1cf7dc21dfa5fa0a615cfa06dc297
statisticsystic.com	255e3db5aa603384d2ca4594b18dc609

f1rst.name	fd90061743e0f33ae5135cb2fbf7057e
tvincoming.com	0c368c121f13928d9699fbc93eead367
f1rst.name	4414e69f4b895551f5a90abb59ff2330
filidaro.com	30ebfdc2a2e90ccd0649ccdf853f1e9d
util4u.com	bc8eb8677390f90de921592c86f17040
util4u.com	3a8455584bda5951b8c0a05deed87b4f
f1rst.name	eb88459f2d532fa3fcc081e2e6a1d549
filidaro.com	008cc983f88b87f8b804988ac4c8d532
mmm-svoboda2012.ru	7a5972a7038f224ff97e02c13082e418
f1rst.name	33d079af33b3689a9d6a9517b39c8d7b
doomns.mooo.com	5190aa75867dde7ca172c2c30d19dcf3
bestkassa.com	4a9fdd47041252608801d16b4ac11e12
162.211.230.170	b4dc51648fa10c349453d80c8cfabed2
nynewsguardianinternet.com	13467f0886de6d0c6716ac0a4eeb2f59
bestkassa.com	c5c05c0f4b9e3b6ac2ad51dc15ef8f43
109.234.35.77	f7a4602db94cd67e9c03d918eaef91a2
78.47.135.84	8b0d8f1d06aea9bc5c7477c9c8284713
5.45.70.137	4c177ad2a07a304318d09fc4ef389a09
194.63.142.171	1a141a76d12f7a310ade141133c0a37c
78.47.135.84	a5aff9aa5b2e45a0f9fea080f8f15971
cdn-rskp.com	1a9b23d9e18c5d19e86fc5a89012a0ef
blackvfl.com	8230f1f93245528c1faa82d945c25332
91.215.155.46	18faa7856fda324ed06261368ab72829
206.su	b7ab83f84103130e46e95de0df8d85a4
206.su	740d9cd8ea165302aa3cd7e6f198ea4c
92.53.96.101	21670682a47021cc4be53ea832df7dbd
91.215.155.46	9079fc3edc31956ab63bbb23673e6c7c
bestkassa.com	1fe21a120f524bb914b210284e1caf05
91.215.155.48	f84928ea5b4752b9cc2a7ae2155d6fd5
178.63.249.40	36f2049cc1a5db224fcd6541d630677f
blackvfl.com	58f1852af6a270d385f270d60d00a0a5
canterus.com	a55149b4164659d5c0e1cd2daef9a702

About the Author

Loucif Kharouni is *a Sr. Threat Researcher at Damballa Inc.* Loucif Kharouni is a Sr. Threat Researcher with Damballa's Threat Research Team. He has been working in the security industry for over 14 years. He has extensive expertise in (OSINT), tracking down cyber criminals, and latest threats campaigns.

His current interests include targeted attacks, financial malware, RATs, PoS malware, bulletproof providers, as well as investigate adversaries and their activities. Loucif has also written many papers and articles regarding computer security and has been interviewed by several industry news publications.

He has participated as a speaker in various cyber crime conferences over the years such as Cert EE, Virus Bulletin, TakeDown Con and ToorCon.

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

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

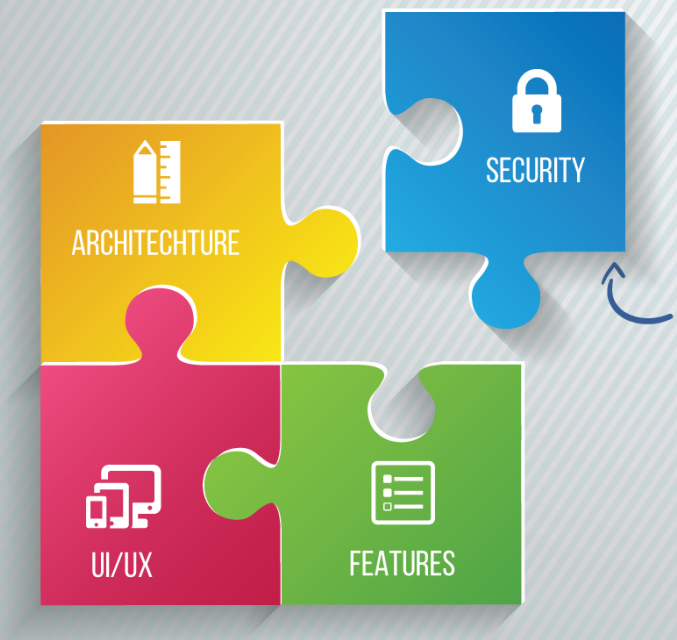
Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY



You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

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

VS.

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

Next thing you know, a discussion ensues and you'll have more than one great answer.

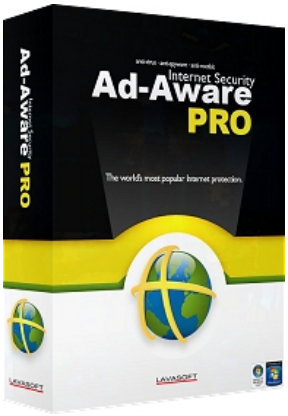
So use it by going here:

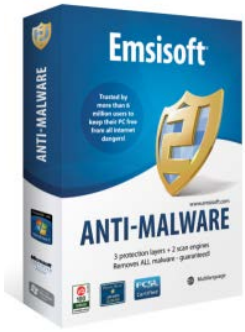
http://www.naisg.org/techtips.asp

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 September 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

Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for September 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…

Online ads used for DDoS after pushing malware

http://www.infoworld.com/article/2986858/network-security/online-ads-used-for-ddos-after-pushing-malware.html

Apple lists top 25 apps hit by malware in first major attack

http://www.reuters.com/article/2015/09/24/us-apple-china-malware-idUSKCN0RO1GR20150924

EXPERTS WARN AGAINST MALWARE THAT CAN DRAIN ACCOUNTS OF ATM USERS IN MEXICO

http://abc13.com/finance/experts-new-malware-can-drain-accounts-of-mexico-atm-users/1002304/

Malware infecting Apple's Apps has already been taken down

http://www.ibtimes.com.au/malware-infecting-apples-apps-has-already-been-taken-down-1469897

Cisco Offers Free Tool To Detect SYNful Knock Router Malware

http://www.darkreading.com/advanced-threats/cisco-offers-free-tool-to-detect-synful-knock-router-malware-/d/d-id/1322332

Intelligent system to check malware hidden in shortened Twitter URLs

http://www.techworm.net/2015/09/intelligent-system-to-check-malware-hidden-in-shortened-twitter-urls.html

Forbes Shuts Down Ads Serving Malware

http://www.forbes.com/sites/thomasbrewster/2015/09/22/forbes-website-served-malware/

Gaza cybergang sending malware files to IT and IR personnel

http://www.scmagazine.com/gaza-cybergang-sending-malware-files-to-it-and-ir-personnel/article/441427/

Hilton hotels in credit-card-stealing malware infection scare

http://www.theregister.co.uk/2015/09/25/hilton_pos_breach/

White House considered bypassing encryption with malware disguised as updates

http://www.theverge.com/2015/9/24/9393091/white-house-break-encryption-updates-working-group

Seven years of malware linked to Russian state-backed cyber espionage

http://arstechnica.com/security/2015/09/seven-years-of-malware-linked-to-russian-state-backed-cyberespionage/

Odlanor Malware Raises Some Concern at PokerStars and Full Tilt

http://www.pokernews.com/news/2015/09/odlanor-malware-pokerstars-full-tilt-22805.htm

Cyber crims up the ante with Google Play brainteaser malware

http://www.theregister.co.uk/2015/09/22/braintest_android_rootkit_brainteaser_malware/

Cardiff University Designs Malware Detection System in Twitter Inc Short URLs

http://www.technewstoday.com/26384-cardiff-university-designs-malware-detection-system-in-twitter-inc-short-ur/

How to Prepare for the Ever-Changing Evolution of Malware

http://www.itbusinessedge.com/slideshows/how-to-prepare-for-the-ever-changing-evolution-of-malware-02.html

How to protect yourself against the XcodeGhost iOS malware

http://www.itworld.com/article/2984944/malware/how-to-protect-yourself-against-the-xcodeghost-ios-malware.html

Hack Brief: Malware Hits 225,000 (Jailbroken, Mostly Chinese) iPhones

http://www.wired.com/2015/08/hack-brief-malware-hits-225000-jailbroken-mostly-chinese-iphones/

Cheetah Mobile Warns About Ghost Push Malware

http://en.yibada.com/articles/67459/20150925/cheetah-mobile-warns-ghost-push-malware.htm

Chinese firm attacks Android phones via malware-laced apps

http://www.v3.co.uk/v3-uk/news/2427186/chinese-firm-attacks-android-phones-via-malware-laced-apps

Malware archaeologist to industry: ‘Enable and configure’ | #splunkconf

http://siliconangle.com/blog/2015/09/24/malware-archaeologist-to-industry-enable-and-configure-splunkconf/

VisitorTracker Malware Affects Thousands of Wordpress Sites

http://www.pcmag.com/article2/0,2817,2491577,00.asp

Kovter malware upgraded with Poweliks features

http://www.scmagazine.com/kovter-malware-upgraded-with-poweliks-features/article/440711/

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

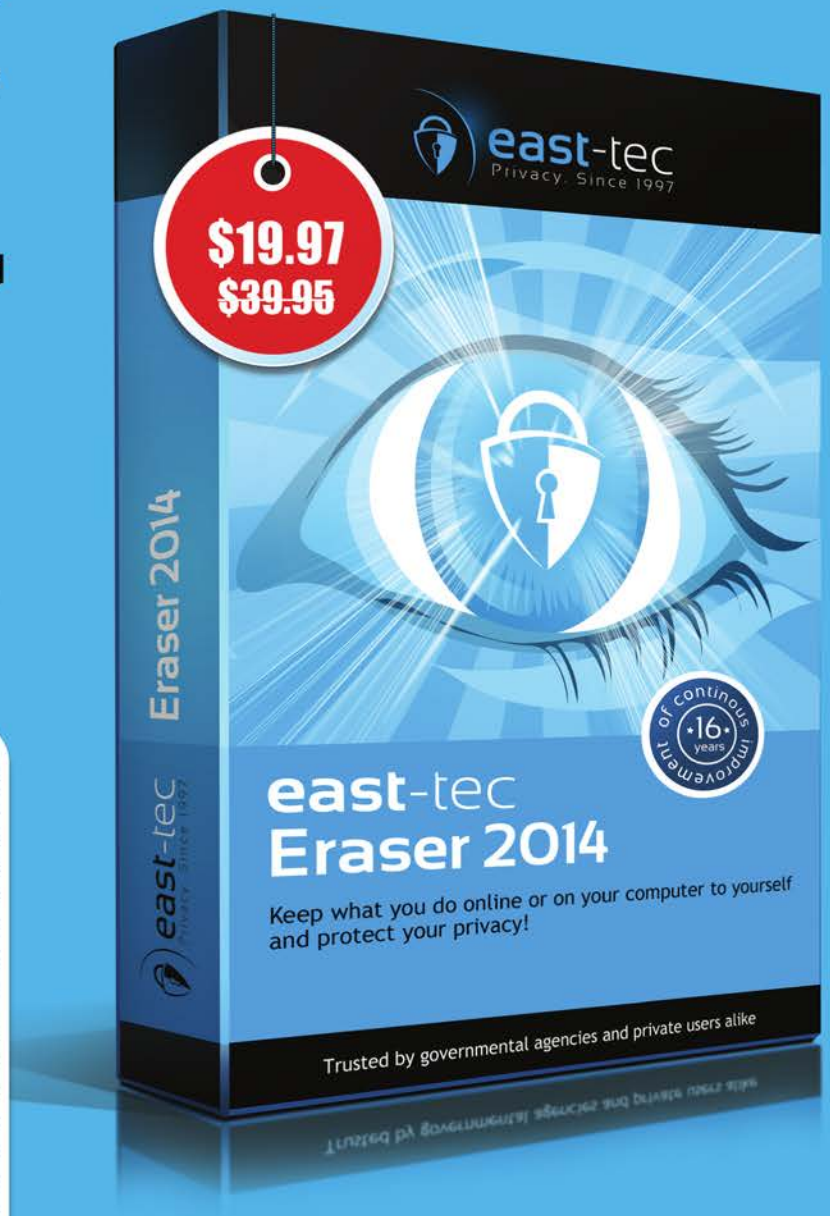
Cyber Defense Magazine - Cyber Warnings rev. date: 09/30/2015

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!



Exclusive offer for Cyber Defense magazine readers

Save 50%

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

Coupon Code:

CYBERMAG2014

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