(IN)SECURE

Issue 43 - September 2014.

WHAT IS THE VALUE OF PROFESSIONAL CERTIFICATION?

THE SYNERGY OF HACKERS & TOOLS AT THE BLACK HAT ARSENAL

USING HOLLYWOOD TO IMPROVE YOUR SECURITY PROGRAM

SECURING THE U.S. ELECTRICAL GRID

MOBILE HACKERS LOOK TO THE NETWORK

TABLE OF CONTENTS

- **Andreas Baumhof**, CTO at ThreatMetrix.
- **John Colley**, Managing Director for EMEA at (ISC)2.
- **Stephen Dodson**, CTO at Prelert.
- **Brian Honan**, CEO of BH Consulting, Founder and Head of IRISSCERT.
- **Adam Maxwell**, Security Researcher.
- **Dwayne Melancon**, Director of Security Research at Lancope.
- **Corey Nachreiner**, Director of Security Strategy and Research at WatchGuard Technologies.
- **Steve Pate**, Chief Architect at HyTrust.
- **Mike Raggo**, Security Evangelist at MobileIron.
- **Giovanni Vigna**, CTO of Lastline.

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@net-security.org
News: **Zeljka Zorz**, Managing Editor - zzorz@net-security.org
Marketing: **Berislav Kucan**, Director of Operations - bkucan@net-security.org

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.

Internet of Things to make CISOs redefine security efforts

By year-end 2017, over 20 percent of enterprises will have digital security services devoted to protecting business initiatives using devices and services in the Internet of Things, according to Gartner. Business cases using Internet of Things (IoT) devices already exist and their role in business and industry will force enterprises to secure them.

Earl Perkins, research vice president at Gartner, said: “IoT security needs will be driven by specific business use cases that are resistant to categorization, compelling CISOs to prioritize initial implementations of IoT scenarios by tactical risk. The requirements for securing the IoT will be complex, forcing CISOs to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security,” Perkins added.

Gartner predicts that the installed base of "things," excluding PCs, tablets and smartphones, will grow to 26 billion units in 2020, which is almost a 30-fold increase from 0.9 billion units in 2009. The component cost of IoT-enabling consumer devices will approach $1, and "ghost" devices with unused connectivity will be common.

There will be a $309 billion incremental revenue opportunity in 2020 for IoT suppliers from delivering products and services. The total economic value-add from IoT across industries will reach $1.9 trillion worldwide in 2020 by which time more than 80 percent of the IoT supplier revenue will be derived from services.

The industries likely to see the greatest value added from the IoT will initially be manufacturing, healthcare providers, insurance, and banking and securities. However, this growth will not be confined there but will expand across all industry sectors.

Phishers resort to AES crypto to obfuscate phishing sites

Phishers have started employing AES encryption to disguise the real nature of phishing sites from automatic phishing detection tools.

This is the latest obfuscating trick in the fraudsters' bag. They have previously used - and still do - JavaScript encryption tools, data URIs and character escaping to achieve the same goal.

Symantec researcher Nick Johnston analyzed the found phishing page (a online banking login page), and explained the procedure: "The page includes a JavaScript AES implementation, which it calls with the embedded password (used to generate the key) and embedded encrypted data (ciphertext). The decrypted phishing content is then dynamically written to the page using document.write(). This process happens almost instantly, so users are unlikely to notice anything unusual."

The used encryption is important for keeping the website under security researchers' radar for as long as possible and to make it more difficult to analyze.

"A casual, shallow analysis of the page will not reveal any phishing related content, as it is contained in the unreadable encrypted text," Johnston noted.

No attempt has been made to hide the key or otherwise conceal what is going on - this is the initial "version" of this obfuscation technique, and will likely not be the final one. Phishing detection will improve, and fraudsters will have to keep pace in order to remain successful.

McAfee and Symantec join Cyber Threat Alliance

Fortinet and Palo Alto Networks, both original co-founders of the industry's first cyber threat alliance, announced that McAfee and Symantec, have joined the alliance as co-founders.

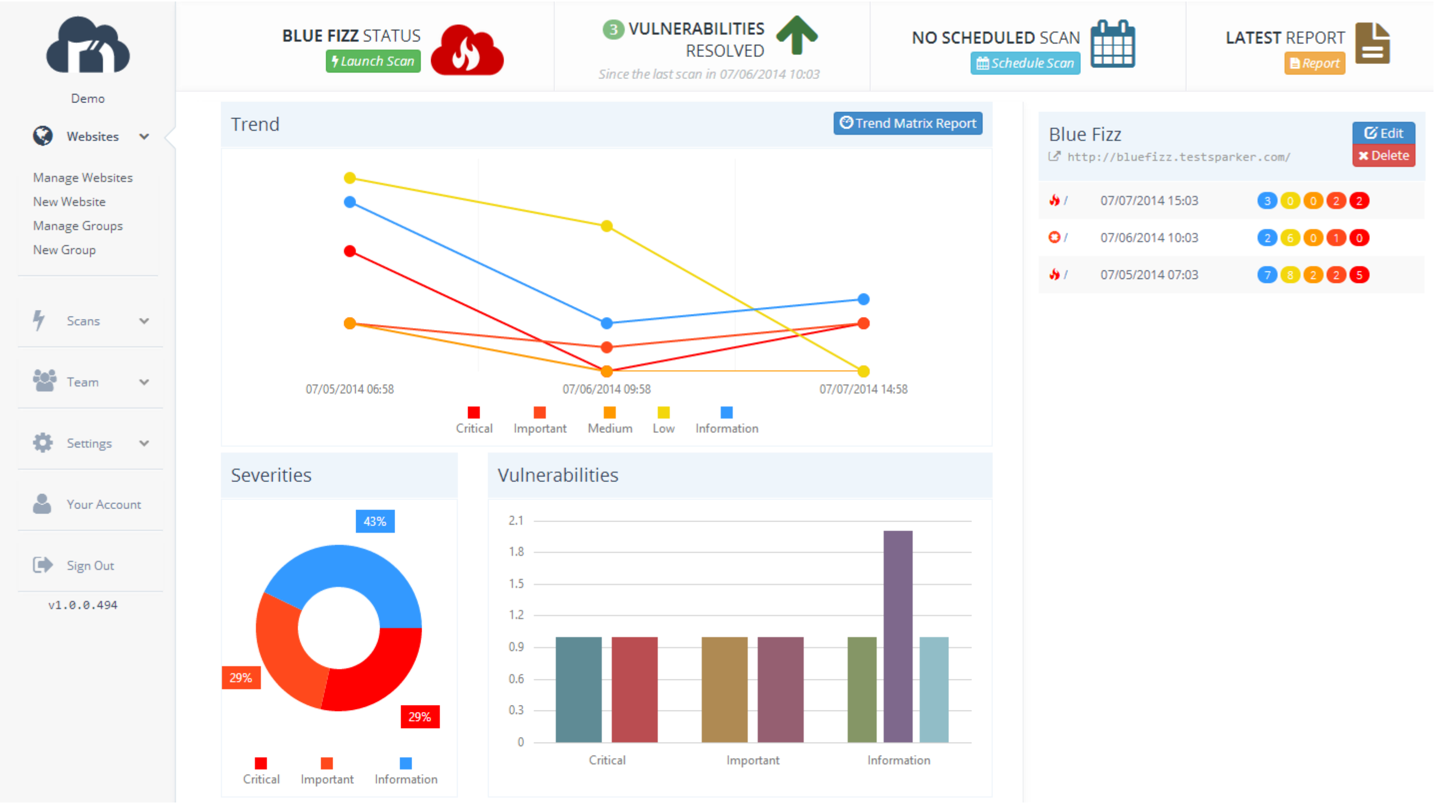
The mission of the Cyber Threat Alliance is to drive a coordinated industry effort against cyber adversaries through deep collaboration on threat intelligence and sharing indicators of compromise.

While past industry efforts have often been limited to the exchange of malware samples, this new alliance will provide more actionable threat intelligence from contributing members, including information on zero-day vulnerabilities, botnet command and control (C&C) server information, mobile threats, and indicators of compromise (IoCs) related to advanced persistent threats (APTs), as well as the commonly-shared malware samples.

By raising the industry's collective actionable intelligence, alliance participants will be able to deliver greater security for individual customers and organizations.

In addition to evolving the alliance framework and bylaws, co-founders Fortinet, McAfee, Palo Alto Networks and Symantec will each dedicate resources to determine the most effective mechanisms for sharing advanced threat data to foster collaboration amongst all alliance members and make united progress in the fight against sophisticated cyber adversaries.

"We must match our adversaries' aggressive drive to innovate with our own deeper commitment to collaborate. It's no longer enough to share and compare yesterday's malware samples. As an industry, we need to understand and be poised to react to the latest complex and multidimensional attacks of today and tomorrow. This cyber alliance provides a critical framework for educating each other on the infrastructure and evolving tactics behind these attacks," said Vincent Weafer, senior vice president for McAfee Labs, part of Intel Security.



A view of Netsparker Cloud

Netsparker announces a new enterprise service offering: Netsparker Cloud

Netsparker announced that their new online security service offering Netsparker Cloud is in its final stages of development and available in Beta.

Netsparker Cloud is an online web application security and vulnerability scanning service built around the already proven false positive free scanning technology of Netsparker, which already helps which already helps thousands of Fortune 500 and world renowned businesses keep their websites and web applications secure.

Netsparker Cloud aims to help large organizations secure their web applications and easily integrate web application security and automated vulnerability scanning in their SDLC. By frequently scanning web applications for vulnerabilities and security issues throughout every stage of the SDLC organizations ensure their web applications are not susceptible to malicious hacker attacks. Netsparker Cloud can scale up and meet the demands and requirements large organizations have. It can scan hundreds and sometimes even thousands of web applications in just a few days. Organizations do not have to build and maintain their own customized and elaborate web application scanning solution since they can rely on Netsparker's expertise of web application security experts.

When using Netsparker Cloud organizations can also benefit from the multi user platform. It is possible to have multiple user accounts with different privileges in Netsparker Cloud, thus allowing for better collaboration between all team members, including developers, QA people and project and product managers. The Netsparker Cloud API allows the remote triggering of automated web security scans and other activities from anywhere, thus easing the process of integrating automated web application security scans in large development environments.

Is your existing cloud based web application security solution meeting all of your organization's requirements and identifying all vulnerabilities? If you'd like a beta account, email contact@netsparker.com.

Surge in cyberattacks targeting financial services firms

Cyberattacks targeting financial services firms are on the rise, but are these organizations doing enough to protect business and customer data?

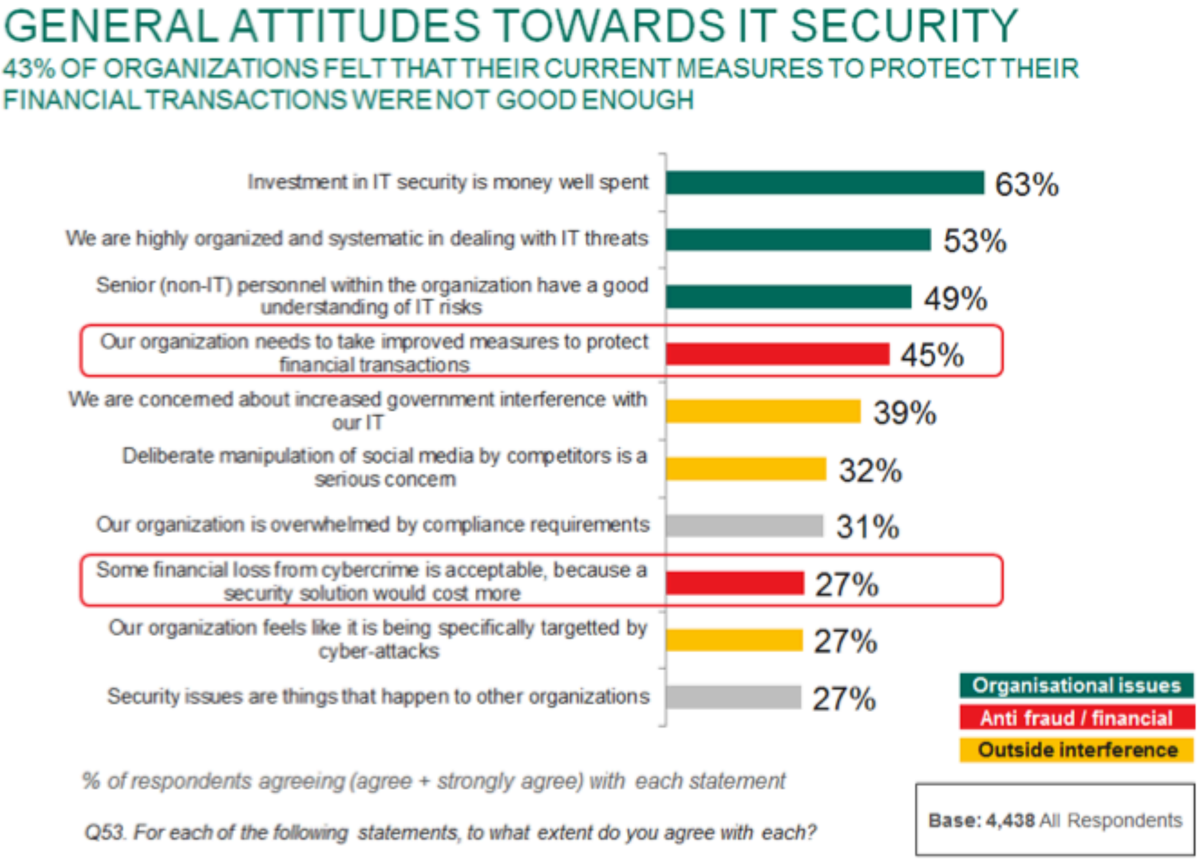
According to a Kaspersky Lab and B2B International survey of worldwide IT professionals, 93% of financial services organizations experienced various cyberthreats in the past 12 months. And while cyberattacks targeting financial services firms are on the rise, nearly one out of three still don’t provide protection of users’ endpoints or implement specialized protection inside their own infrastructure.

According to the survey, this lack of action to protect themselves from an attack is causing many businesses to lose faith in financial firms tasked with keeping their information safe. In fact, only 53% of businesses felt that financial organizations did enough to protect their information. The survey also found that 82% of businesses would consider leaving a financial institution that suffered a data breach and that 74% of companies choose a financial organization according to their security reputation. This sentiment was echoed in a separate Kaspersky Lab Consumer Security Risks survey that found that 60% of consumers prefer companies that offer additional security measures to protect financial data.

The clear divide between what a business expects from a financial institution versus common perceptions toward the damage caused from a data breach is magnified further when you take into account that only 28% of financial services organizations think that the risk of damages from cybercrime is outweighed by the cost of prevention.

This mindset is particularly flawed given that 52% of financial institutions have a policy of reimbursing all losses caused by cybercrime without investigation and that the true cost of financial data loss is between $66,000 - $938,000 depending on the size of the organization.

However, the Kaspersky Lab survey uncovered a glimmer of hope for financial services organizations’ eventual turn toward implementing adequate security. 47% of financial companies think that loss of credibility/damage to reputation as a result of a data breach is the worst consequence to the company.


GENERAL ATTITUDES TOWARDS IT SECURITY

43% OF ORGANIZATIONS FELT THAT THEIR CURRENT MEASURES TO PROTECT THEIR FINANCIAL TRANSACTIONS WERE NOT GOOD ENOUGH

% of respondents agreeing (agree + strongly agree) with each statement

Q53. For each of the following statements, to what extent do you agree with each?

Base: 4,438 All Respondents

Twitter launches bug bounty program

With a simple tweet, Twitter has officially launched its own bug bounty program.

Set up through the security response and bug bounty platform HackerOne, the program offers a minimum of $140 per threat. The maximum reward amount has not been defined.

The company is currently asking bug hunters to submit reports about bugs on its Twitter.com domain and subdomains (ads.twitter.com, apps.twitter.com, tweetdeck.twitter.com, and mobile.twitter.com) and its iOS and Android apps.

"Any design or implementation issue that is reproducible and substantially affects the security of Twitter users is likely to be in scope for the program," the company pointed out. "Common examples include: Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Remote Code Execution (RCE), unauthorized access to protected tweets, unauthorized access to DMs, and so on."

Reports about bugs on other Twitter properties or applications are welcome, but will not be eligible for a monetary reward - bug hunters will have to be content with a mention on the Twitter's Hall of Fame, which is already populated with the names of 44 hackers. In fact, Twitter's bug reporting program on HackerOne has been up for three months now, but the company has only now announced that it will start paying out bounties.

So far, 46 of the reported bugs have been closed by the company's security team, but reports received prior to September 3, 2014, are also not eligible for monetary rewards.

"Maintaining top-notch security online is a community effort, and we're lucky to have a vibrant group of independent security researchers who volunteer their time to help us spot potential issues," the company noted, adding that the bug bounty program was started to "recognize their efforts and the important role they play in keeping Twitter safe for everyone."

80% of business users are unable to detect phishing scams

McAfee Labs revealed that phishing continues to be an effective tactic for infiltrating enterprise networks.

Testing business users' ability to detect online scams, the McAfee Phishing Quiz uncovered that 80% of its participants failed to detect at least one of seven phishing emails. Furthermore, results showed that finance and HR departments, those holding some of the most sensitive corporate data, performed the worst at detecting scams, falling behind by a margin of 4% to 9%.

Since last quarter's Threats Report, McAfee Labs has collected more than 250,000 new phishing URLs, leading to a total of nearly one million new sites in the past year. Not only was there an increase in total volume, there was a significant rise in the sophistication of phishing attacks occurring in the wild.

Results showed both mass campaign phishing and spear phishing are still rampant in the attack strategies used by cybercriminals around the world. Meanwhile, the United States continues to host more phishing URLs than any other country.

“One of the great challenges we face today is upgrading the Internet's core technologies to better suit the volume and sensitivity of traffic it now bears,” said Vincent Weafer, senior vice president for McAfee Labs. “Every aspect of the trust chain has been broken in the last few years—from passwords to OpenSSL public key encryption and most recently USB security. The infrastructure that we so heavily rely on depends on technology that hasn't kept pace with change and no longer meets today's demands.”

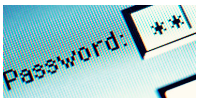
Acunetix offers free network security scan

Acunetix is offering 10,000 free network security scans with Acunetix Online Vulnerability Scanner (www.acunetix.com/free-network-vulnerability-scan) in a bid to make it easier for businesses to take control of their network security. This is a hosted security scanner that will scan a perimeter server for network level vulnerabilities and provide detailed reports so as to allow the security administrator to fix the vulnerabilities before a hacker finds them.

All the network scanning capabilities available in Acunetix OVS will be available for free for fourteen days, allowing users to audit their internet (and hacker) facing servers. The free network scan feature allows companies to:

- Scan their servers for over 35,000 network vulnerabilities
- Audit their internet facing servers and identify system and network weaknesses
- Ensure that servers are not running any illegitimate services, such as Trojans, or services that are installed unintentionally
- Identify any vulnerable versions of applications running on the servers
- Discover the information that the systems are leaking using various techniques such as OS fingerprinting, port banner grabbing and service probing
- Get additional information about other vulnerabilities and network problems detected.

Give up on complex passwords, says Microsoft



Do password composition policies work? Does forced password expiration improve security? Do lockouts help protect a service? What do password meters accomplish? These are just some of the questions a group of researchers from Microsoft and the Carleton University in Canada wanted to find answers to.

"Despite long-known shortcomings in both security and usability, passwords are highly unlikely to disappear," they pointed out in a recently released paper. So, they took it upon themselves to survey existing literature, and by using "ground-up, first-principles reasoning," they have apparently discovered what works and what doesn't.

According to the researchers, users usually put accounts in different categories, mostly based on the potential consequences of an account compromise.

On one end of the spectrum are the accounts that users consider unimportant and can choose weak passwords for. On the other are the critical accounts they want to protect as best they can because they contain information they don't want to lose or have revealed, or are critically tied to other accounts, and for which they often choose complex passwords and additional protection options (such as multi-factor authentication).

For users, it's important not to use the same password for accounts in different categories. And web admins should try to determine in which of theses categories their site falls into, and choose a password scheme and storage option accordingly.

"We should not be quick to express outrage on learning that password1 and 123456 are common on publicly-disclosed password lists from compromised sites, if these are don't-care accounts in users' eyes. Nor should it be surprising to find passwords stored cleartext on fantasy football sites," the researchers say.

Among the things that the researchers discovered is that fact that password strength meters are practically useless, and so are the usual suggestions for making a longer and more complex password.

They pointed out that password that will withstand online and offline password guessing attacks are different, and that "attempts to get users to choose passwords that will resist offline guessing, e.g., by composition policies, advice and strength meters, must largely be judged failures."

Expert international cybercrime taskforce tackles online crime

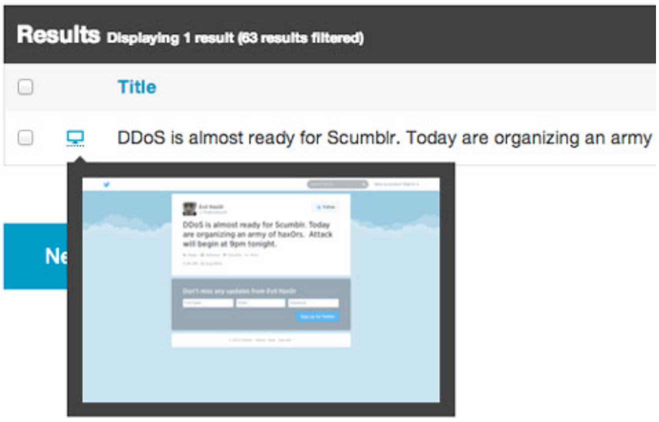
Hosted at the European Cybercrime Centre (EC3) at Europol, the Joint Cybercrime Action Taskforce (J-CAT), which is being piloted for six months, will coordinate international investigations with partners working side-by-side to take action against key cybercrime threats and top targets, such as underground forums and malware, including banking Trojans.

The J-CAT will be led by Andy Archibald, Deputy Director of the National Cyber Crime Unit from the UK's National Crime Agency (NCA).

Key contributors to the intelligence pool will be the EU Member States via EC3, and other law enforcement cooperation partners. Thus far, Austria, Canada, Germany, France, Italy, the Netherlands, Spain, the UK and the US are part of the J-CAT. Australia and Colombia have also committed to the initiative.
Troels Oerting, Head of the European Cybercrime Centre says: “For the first time in modern police history a multi-lateral permanent cybercrime taskforce has been established in Europe to coordinate investigations against top cybercriminal networks. The aim is not purely strategic, but also very operational. The goal is to prevent cybercrime, to disrupt it, catch crooks and seize their illegal profits."

"This is a first step in a long walk towards an open, transparent, free but also safe Internet. The goal cannot be reached by law enforcement alone, but will require a consolidated effort from many stakeholders in our global village. But the J-CAT will do its part of the necessary ‘heavy-lifting’ and that work started today. I am confident we will see practical tangible results very soon," Oerting added.

Netflix open sources tools for detecting planned attacks



Results Displaying 1 result (63 results filtered)

Title

DDoS is almost ready for Scumblr. Today are organizing an army

Making good on their word to open source many of their internally developed tools and libraries, Netflix has released three new tools that allow security teams to keep an eye out for Internet-based discussions regarding potential attacks against their organization's infrastructure, whether it's DDoS attacks or any other kind.

The tools are named Scumblr, Sketchy and Workflowable. Scumblr is an app that trawls the Web for posts and discussions that mention attacks or any other content of interest.

"Scumblr includes a set of built-in libraries that allow creating searches for common sites like Google, Facebook, and Twitter. For other sites, it is easy to create plugins to perform targeted searches and return results," Andy Hoernecke and Scott Behrens of the Netflix Cloud Security Team explained. "Once you have Scumblr setup, you can run the searches manually or automatically on a recurring basis."

Scumblr uses Workflowable to set up workflows triggered by the different nature of search results, automating - at least in part - the defenders' reaction.

Sketchy can also be integrated with Scumblr. Its purpose is to automatically make screenshots of the found conversations and statements, scrape the text, and save HTML so that even it all of it gets removed in time, the screenshots remain as evidence, and security analysts can preview Scumblr results without having to visit the potentially malicious sites directly.

What is the value of professional certification?

by John Colley

Recognition for and therefore the value of professional certification is rising within the information security domain. In an increasing number of markets across Europe, chances are that if there is a job being advertised that requires someone to ensure information security of systems, data, software, or the company overall, they will be asked to demonstrate at least a baseline of practical knowledge by having earned a professional certification in the field.

This is a reflection of the growing appreciation on the part of the employers that commonly understood best practice approaches and methodology for information security actually exists, and of the increasing dependency on it as companies and governments become ever more reliant on connected and therefore besieged IT systems.

It is also a recognition of the serious nature of the responsibilities that come with the job - responsibilities that justify the application of professional standards to the task, as the potential impact of getting it wrong can be devastating.

Documenting practice

It is important to note that professional certification is not about gaining a certificate after the completion of a training course. Certification can more accurately be described as a form of standardization as it federates recognition for practice knowledge.

When individuals pursue professional certification, they are verifying their skills and abilities that more often than not have been developed over time through professional development and on-the-job experience. Training is optional and on its own for the uninitiated will not be enough to achieve a professional-level certification.

REGULAR ROBUST ASSESSMENT ENSURES HOLDERS OF THE CERTIFICATE CAN CONTINUE TO PROVIDE INSTANT ASSURANCE THAT THEY POSSESS THE MOST UP TO DATE, REAL-WORLD KNOWLEDGE REQUIRED IN THEIR FIELD.

People become certified professionals by passing a rigorous examination and receiving the endorsement of their colleagues with respect to their practical experience.

(ISC)2 was formed 25 years ago, as a not-for profit membership body, with the objective of establishing broad recognition for practice knowledge. The goal was to both document grass roots experience and create a structure for maintaining the currency of this on-the-job knowledge over time.

Today over 20,000 of our globally 100,000 certified members from around the world regularly participate in the biannual Job Task Analysis surveys we conduct to maintain all of our certifications. Also, as the need for security develops, our members have similarly influenced the development of new areas of certification.

In the last 12 months, we have established certifications for the Healthcare Information Security and Privacy Practitioner (HCISPP) and the Certified Cyber Forensics Professional (CCFP).

The value of any professional certification lies in the rigor applied to ensure its continued relevancy. Regular robust assessment ensures holders of the certificate can continue to provide instant assurance that they possess the most up to date, real-world knowledge required in their field. It is also an assurance that they can communicate using, and work under, the same terms and concepts as colleagues working all over the world.

This assurance comes from the fact these concepts have been tried, tested and verified to represent best practice through the experience of thousands working in the field.

These are basic maxims that we generally associate with professions that have been established for many years, such as engineering, accounting or architecture.

An asset to society

The need becomes quite obvious when you consider the challenges faced without the foundations of recognized professional practice, particularly in fields of practice that carry significant levels of responsibility.

In healthcare, for example, there has always been a recognition for the sensitive nature of data and the need to keep it secure, yet in recent years this has become a sector where reported breaches are prolific.

The move away from paper-based processes and the emergence of what has become known as “Connected Healthcare” requires a whole new set of data governance measures that must be understood across the various organizations and suppliers that now interact with front-line healthcare providers.

Often for very legitimate reasons many organizations have access to records that would have previously been inaccessible because they could only have been viewed in person. The healthcare industry is therefore in the process of redefining the norms that can uphold its ingrained respect for privacy.

In the absence of comprehensive national-level or international good practice standards, vulnerabilities have emerged, breaches have become numerous and public trust has waned. This became obvious when the United Kingdom’s NHS Care.data scheme aimed at creating a central database for healthcare records was officially stalled earlier this year.

The public backlash at the request of a whole population to give consent to allow the transfer of their sensitive health information, previously only known to individuals at a local Primary Health Care Trust, to a centralized database, caused uproar with UK Parliamentarians. The HCISPP is the response to this and similar scenarios around the world by subject matter experts who work within healthcare and understand the value of sharing the lessons they learned and establishing a relevant baseline of knowledge for information security and privacy.

It's a value that also translates to governments and their policy makers who seek to regulate for our safety and economic well-being.

Governments are becoming particularly active in the cyber-security arena as awareness of the nature and impact of cyber threats develops.

They must draw on the best information available, and a professional certification body with its privileged access to a wealth of front-line knowledge has a significant contribution to make. As a result, the certification bodies and their professional community are becoming an asset to society in general, getting involved in community awareness, consultation on standards and cyber security strategy, skills frameworks, academic development, and cyber security capacity building in underdeveloped countries.

CERTIFICATION INCREASES SELF-EFFICACY BY AFFECTING CONFIDENCE AND THE APPROACH TO GOALS, TASKS, AND CHALLENGES WITHIN THE WORKPLACE.

The career move

When an individual chooses to become a certified professional their initial instinct is usually to further their career and earn a higher salary.

There is a reasonable body of research within Europe's largest markets that demonstrates a link between greater recognition of the value of certification with increased earnings and career potential. In fact, the now widely-acknowledged skills gap for people with cyber security skills and competency ensures that those with certifications face strong prospects.

Once certified, the motivational factors deepen, as the individual becomes part of a recognized community. For most professionals, this increases their belief that they can achieve success in their job role and encourages self-worth.

This self-efficacy – an internal belief that they have the ability, knowledge and skills to succeed in specific situations just as their peers or seniors have – is invaluable.

Certification increases self-efficacy by affecting confidence and the approach to goals, tasks, and challenges within the workplace. It also facilitates resilience, instils persistence and a determination to succeed despite the obstacles faced in their professional lives – because they are secure in their capability and knowledge.

Further, professional certifications have to be maintained. Professionals have to pursue continual learning by earning continuing professional education credits in order to retain their certification.

By continuously updating their knowledge, professionals are better placed to both create and identify opportunities for success, and proactively move their career forward. They are better able to apply the learned knowledge and in turn improve their skills and expertise to more effectively perform their job functions. For their employers, this translates into a stronger business, better able to achieve its strategic goals and objectives.

WHILE OFTEN MISUNDERSTOOD, PROFESSIONAL CERTIFICATION HAS PROVEN TO BE AN EXTREMELY EFFECTIVE MECHANISM IN A FAST–CHANGING WORLD.

The commitment

When I first became a Certified Information Systems Security Professional (CISSP) with (ISC)2 in 1998; I was one of only a few in the United Kingdom and Europe to have done so.

At the time, few employers recognized this new credential. The salary and career benefits were not as obvious as they can be today. Despite this, the pursuit of my credential still clearly communicated commitment to achieve the certification, sign up to a professional code of ethics and maintain currency. In short, it communicated commitment to being a professional.

This is a value that I and many of my colleagues perceived as hiring managers, and one which I believe has strongly contributed to the ensuing development of professional certification across Europe.

I remain passionate about the development of this value, responding to members' commitment as well as their clear desire to be active in the effort to move the profession forward.

In summary, while often misunderstood, and not necessarily the only solution available for the development of skills and knowledge in cyber or information security, professional certification has proven to be an extremely effective mechanism in a fast–changing world.

By providing a vehicle by which knowledge, skills and experience can be broadly shared and also validated, certification has helped the world develop a much needed capacity to defend against very new, evolving and all-too-often poorly understood threats in a relatively short period of time. I believe this is a value that is very difficult to quantify, yet increasingly easy to appreciate.

John Colley, CISSP, is Managing Director for EMEA at (ISC)2 (www.isc2.org). (ISC)2 is the largest membership body of information security professionals, and the administrator of the CISSP, with nearly 100,000 certified members worldwide, including more than 16,000 working across Europe Middle East and Africa.

6'0"
5'6"
5'0"

How to tell if your security system has been fingerprinted by evasive malware

by Giovanni Vigna

Earlier this year, Symantec proclaimed that AV was dead. A report from Lastline Labs indicated AV hadn't died or been rendered entirely useless, it just couldn't keep up with the onslaught of advanced malware flooding connected systems.

Each day newly detected malware got past as much as half of the antivirus vendors. Somewhat shockingly, even after two months one third of the AV scanners were unable to detect many malware samples. In some cases, the least detected 1-percentile of malware was never detected at all.

But AV evasion is relatively easy for advanced malware authors. Many malware samples are polymorphic, meaning they self-encrypt, changing their executable image, so that a static signature-based detection model like that of traditional AV doesn't recognize the code as malicious and lets it through.

In response, organizations have started implementing emulated or virtualized sandboxing technology to conduct behavioral analysis of unrecognized code entering their networks as email attachments or web downloads. This allows for a safe, isolated environment in which to observe the actions of the code before determining its threat level.

Because dynamic analysis looks deeper into the behavior of the code rather than simply looking for known threats based on signatures, it can identify and block new threats before a signature can be generated and distributed by traditional AV vendors.

The advantage of this type of analysis (technically called "dynamic analysis") is that it does not matter how the code looks: the only thing that matters is what the code does. Therefore, models of malicious behavior can be used as a general way to detect entire families of malware, without having to rely on brittle and soon-outdated static signatures.

Advanced malware authors are also catching on to these emulated or virtualized dynamic analysis environments that are increasingly popular complements to signature-based detection in public and private sector security deployments. For example, malware samples troll for registry keys, processes, functions and IP addresses that allow them to fingerprint the analysis tool itself. If evasive malware detects an analysis environment, it can cloak itself, abort the mission or stall for several minutes until the analysis is over.

In fact, dynamic malware analysis is usually more resource-intensive than static analysis, and each sample can be executed for a few minutes only, if one wants to analyze large amount of samples each day (often tens or hundreds of thousands). As a result, stalling (by suspending or by looping) can be effectively used to bypass dynamic analysis.

In essence, malware authors are fingerprinting security systems and evading their detection capabilities. How, then, do you know if your system has landed in malware authors' fingerprint database? How is it possible to distinguish a benign sample that does not perform any harmful action from a malicious - yet evasive - one that pretends to be harmless because it has "sensed" its execution environment?

Recent research conducted and presented at the 23rd USENIX Security Symposium by Dhilung Kirat, PhD Candidate at UCSB (in collaboration with fellow Lastline co-founder and UCSB professor Christopher Kruegel and myself) indicates that you can identify evasive malware by observing it in multiple environments to determine if it behaves differently.

This system, called BareCloud, lets you look for malware that has "multiple personalities." This is because programs are usually mostly deterministic. This means that given very similar execution environments and identical inputs, they most likely behave in the same manner. So, if a program's behavior diverges widely in different (yet similar) execution environments, it might be the case that this difference in behavior is associated with malicious intent. In practice, a key technique in detecting evasive malware is to use the evasive behavior of a program as a "signal" to identify that the program is malicious.

Dhilung Kirat's research focuses on creating a system that can automatically pick up this "signal," so that the evasive malware can be identified and studied by the developers of anti-malware solutions to improve their analysis techniques.

The basic idea is very simple: execute a malware sample in several virtualized analysis environments (or "sandboxes") and compare the observed behaviors to the execution of the same sample on a real machine, installed with the Windows operating system, and without any modifications, which mimics a real victim machine (this set up is called "bare metal" as the sample is run on the actual hardware CPU, without any virtualization).

If the malware sample behaves maliciously in the bare metal environment but is silent when executed in one or more of the virtualized ones, it means it has some fingerprinting and evasion capability.

Of course, running malware on bare metal comes with a number of challenges. First of all, restoring the analysis system after a malware sample infects the machine is very easy in virtualized environments, which can take "snapshots" of their clean image. This, however, is much more difficult in a bare metal system where no snapshot mechanism exists. Therefore, we had to develop some techniques to restore the execution environment in an efficient way. For example, we used external SCSI disks that allowed us to transparently intercept modifications to files and discard them at the end of the analysis, returning the disk to its original configuration.

The second challenge is comparing the behavior collected in the various analysis environments. In fact, each system has its own way of providing information about what a malware sample did.

In addition, even though bare-metal analysis systems are usually able to extract more behavior out of malware samples, the details of the behavior are very limited, as there is no instrumentation that can extract low-level traces of malware behavior (that's why the system is called "bare"). Therefore comparing the coarse-grained behavior reports of bare-metal analysis with the fine-grained reports produced by virtualized environments is a challenge.

To address this problem, we developed a novel comparison algorithm in BareCloud that allows us to efficiently identify samples that have "multiple personalities."

The algorithm is based on a hierarchical similarity-based approach that is well suited for the analysis of event traces at different levels of abstraction and granularity. More precisely, instead of looking at the events produced without any differentiation, the algorithm first creates a high-level representation that is common across all analysis systems.

This representation models the types of objects being modified (e.g., files), the type of operation being performed (e.g., creation of a file), and the actual parameters of the operation (e.g., the name of a file). Then, the algorithm organizes these components in a hierarchy and performs similarity analysis at matching level in each hierarchy.

This approach has several advantages, and it is particularly well suited to identify deviations associated with evasive behavior.

Of course we first needed to have behaviors that are as comparable as possible. For example, if we would have executed the sample at different times on the different platform, the time might have affected its behavior regardless of the malicious or evasive nature of the sample. Therefore, another challenge was to synchronize the execution of the same sample on different environments. Precisely controlling the behavior deviation introduced by the external environment is difficult. This is because these factors are not always under our direct control. However, failure to minimize the impact of these factors may result erroneous behavior deviations. This consideration is important because most malware communicates with the external environment to carry out its malicious activities. To minimize the effect of the external environment, we implemented the following strategies:

1. Synchronized execution: We execute the same malware sample in all analysis environments at the same time.

2. Identical local network: We expose all analysis systems to identical simulated local network environments.

3. Network service filters: To minimize the non-determinism introduced by different network services, we actively intercept network communications and maintain identical responses to identical queries among all instances of a malware sample running in different analysis environments.

Stemming from this research, we witnessed some key attributes of both the evasive malware and the dynamic analysis environments that the sample attempted to evade.

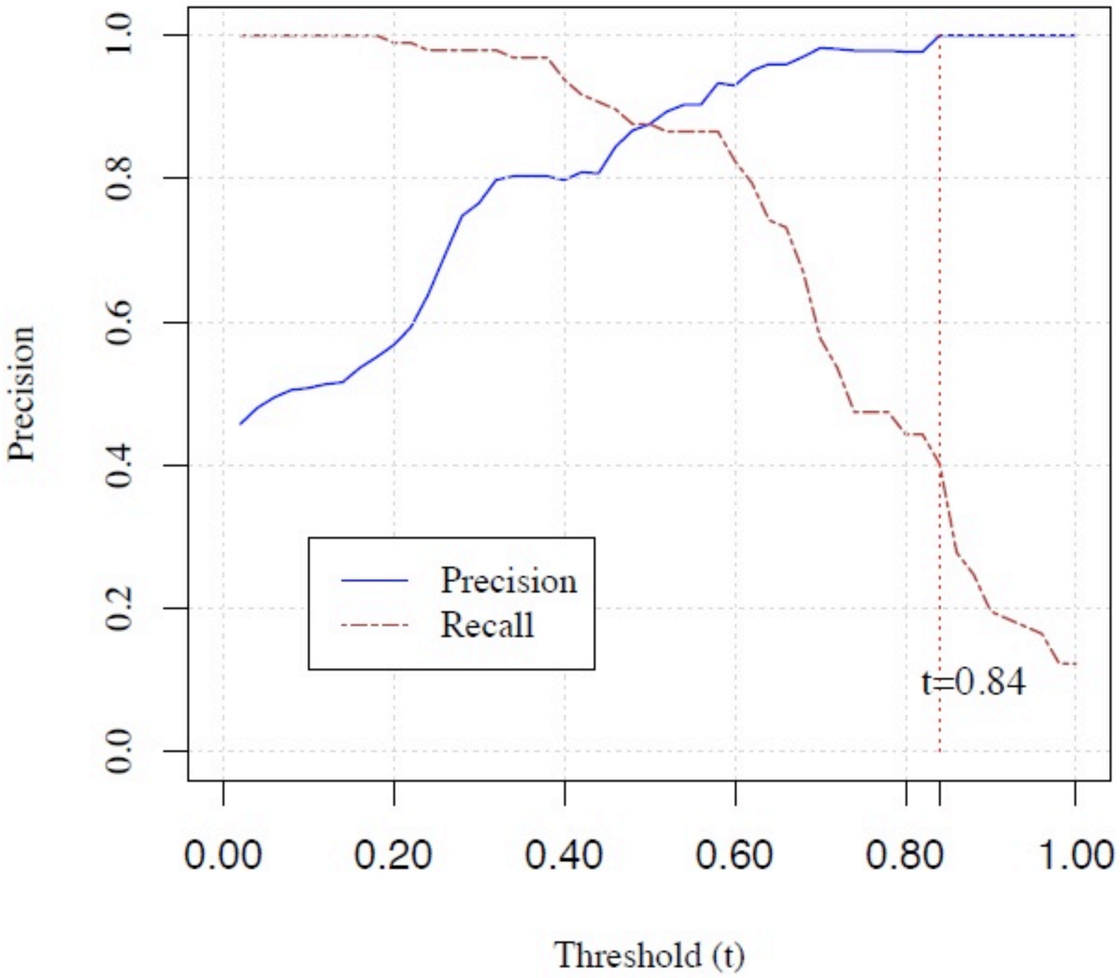
This lends new insights into how to detect evasive malware leveraging bare-metal analysis (as opposed to in a virtualized environment) and prevent the malware from sensing its quarantined test environment, and/or expose the malware sample's stealthy nature.

As with any security tool, tuning the sensitivity to optimize for precision and accuracy is crucial. If the system is too sensitive and the noise is overwhelming, malware authors can hide malicious behavior in this noise. If the system is not sensitive enough then a large volume of malicious code gets through undetected. We found experimentally that there is a "sweet spot" in the sensitivity of the system that allows for almost zero false positives with a good detection rate.

Since the goal of the system is to serve as a filtering step to identify malware samples to be further analyzed by a human, the precision of the system is the most important factor, as a mistake (that is, identifying a sample as evasive when it's actually not evasive), might cost many expensive man-hours. Therefore, we chose a threshold for our algorithm that would maximize our ability to correctly identify samples (at the cost of missing some).

You can see it depicted in the chart on the following page at t=0.84. This threshold is a parameter of our algorithm that is able to describe when two behaviors have to be considered really "deviating" from each other.

Ultimately, we determined that a substantial fraction (~5.3%) of the malware samples were evasive, which indicates a significant trend in malware actively fingerprinting and evading sandboxing environments.

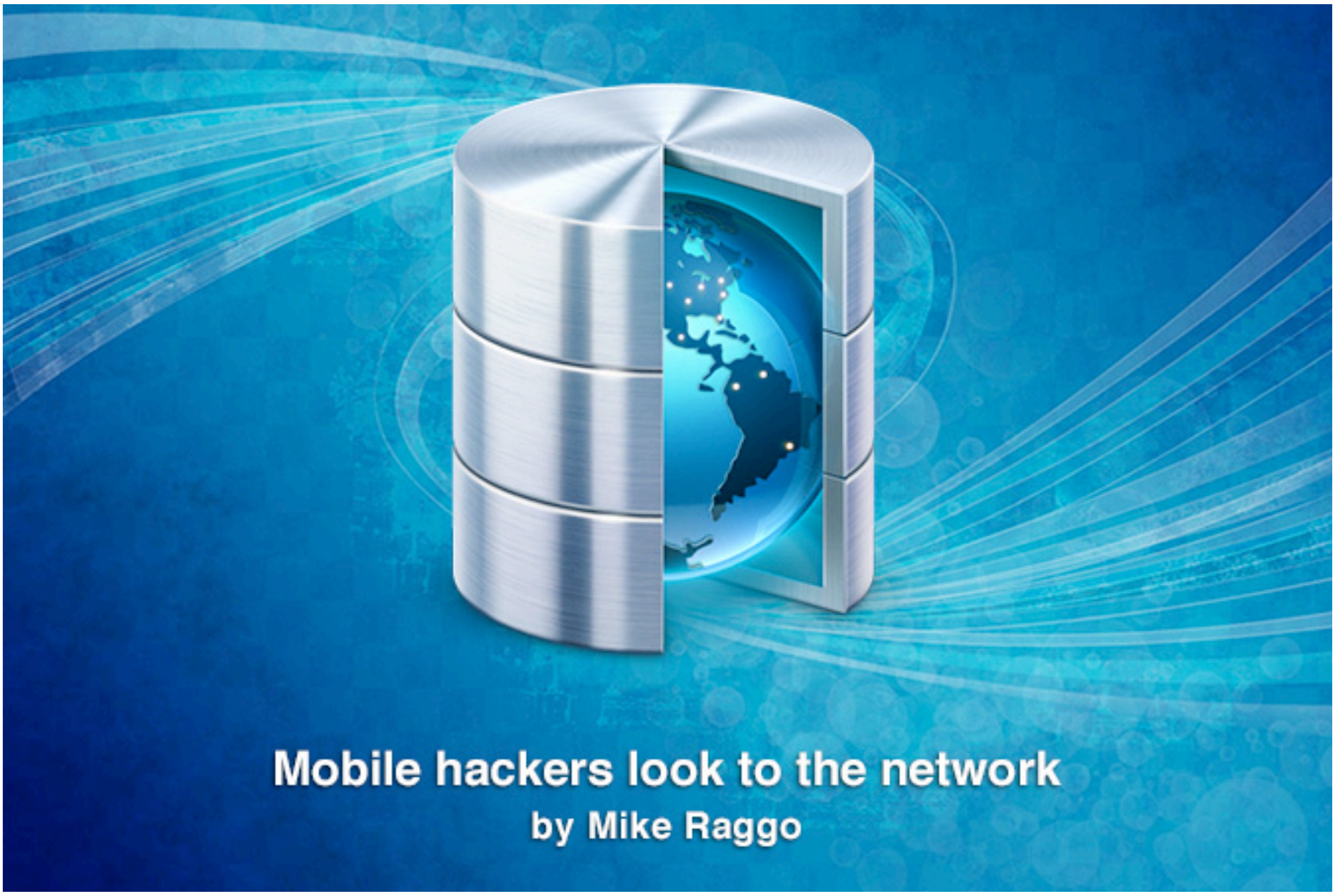


Systems like BareCloud can keep an eye on the evasive malware trend and identify malware samples that effectively evade current systems. These samples can be then analyzed in more detail by human analysts, who can then devise countermeasures to prevent fingerprinting and detect the evasive behavior within the sandbox. This is an important step in the arms race, as it forces the malware author to invest a substantial amount of effort in devising novel evasion techniques.

In the world of malware authors, time is money and any added complexity in exploiting a system reduces the profitability and therefore diminishes the incentives for cybercriminals to continue attacks against well secured targets. It is important to emphasize though that our research indicates that about 1 in 20 malware samples performed maneuvers that evade virtualized sandboxing technologies. That's not a trivial proportion when you consider the rising tide of malware bombarding organizations and individuals today. And these samples were from one year ago, so it is very likely that it's even greater now.

This research serves as a wake up call to both the research community and the security technology sector: evasive malware is here and is effectively defeating existing security systems - including virtualized sandboxing - on a regular basis. Therefore, we need innovation in this field to stay ahead in the arms race.

Giovanni Vigna is co-founder and CTO of Lastline (www.lastline.com) as well as Professor of Computer Science at UCSB. He has been researching and developing security technology for more than 20 years, working on malware analysis, web security, vulnerability assessment, and intrusion detection. He is known for organizing and running an annual inter-university Capture The Flag (iCTF) hacking contest that involves dozens of institutions and hundreds of students around the world.



Mobile hackers look to the network

by Mike Raggo

Choice is messy. When it comes to our choice of technology at work, specifically mobile apps, content and devices, that mess is mostly handled by the IT department. And between the network, the devices and the data on them, they have plenty to worry about.

Users can download the apps of their choice, connect to cloud services of their choice, and even connect to networks of their choice.

From a network perspective, this makes mobile devices low-hanging fruit for attackers. When employees travel, for example, we know they are going to connect to open wireless networks at coffee shops, hotels, and airports. This provides hackers with the perfect opportunity to target wireless devices.

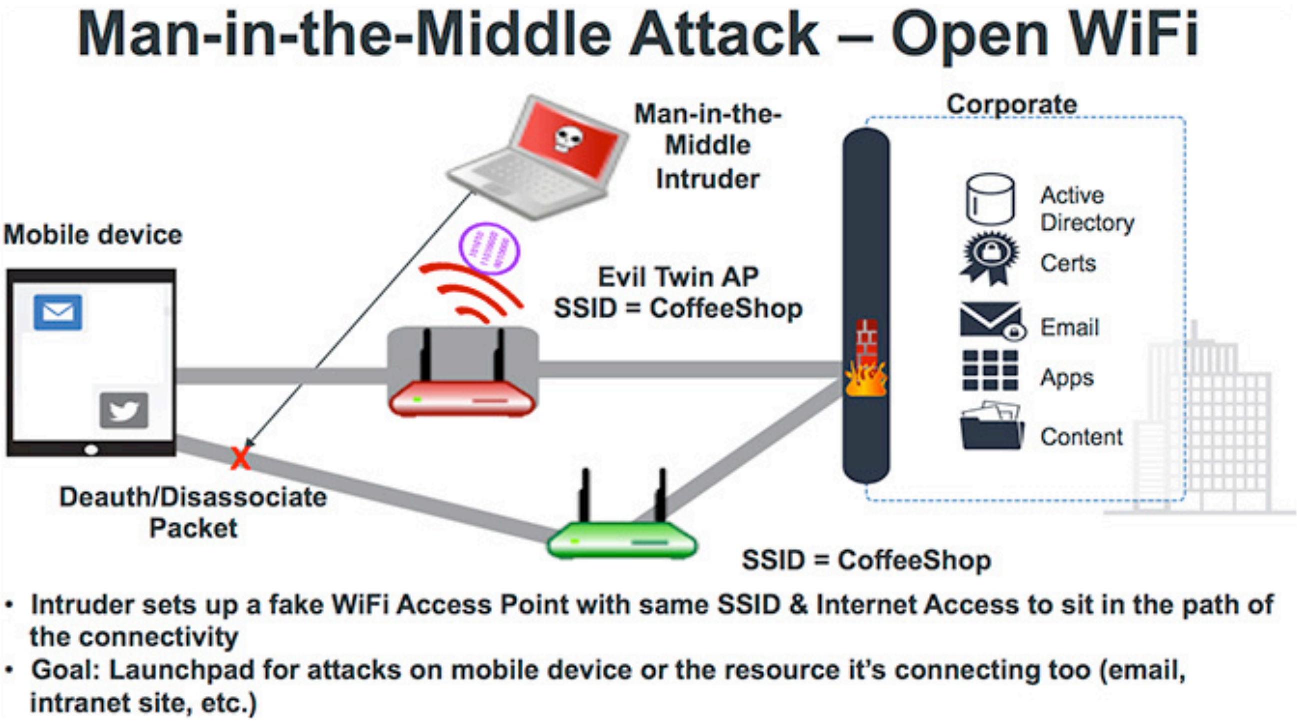
Anatomy of an attack

Wireless sniffing can be performed without connecting to the WiFi in a more passive mode at Layer 2 of the TCP/IP stack. Some profiling information, such as MAC addresses, SSIDs, and leaking layer 2 broadcast protocols such as NetBIOS, STP, VRRP, HSRP, can be gathered in this manner.

When an attacker connects to the open WiFi, he/she can collect arguably more valuable information and data at Layer 3 and above. The simplest approach is an interception attack, which enumerates encrypted and unencrypted connectivity. Usernames, passwords, email content, and other data are exposed when unencrypted.

Attackers also like to target encrypted data. To accomplish this they may leverage a device armed with Kali or Backtrack Linux distributions, or a purpose-built box like a WiFi Pineapple. All of these allow attackers to set up their own wireless access point or an open WiFi, usually with the same SSID.

This fake access point (AP) can either attract unwary users or knock users off the legitimate open WiFi and get them to connect to the fake AP. This fake AP also provides Internet access, so the user has no idea he's now connected to a malicious access point.



Man-in-the-Middle Attack – Open WiFi

Man-in-the-Middle Intruder

Corporate

Mobile device

Evil Twin AP
SSID = CoffeeShop

Active Directory

Certs

Email

Apps

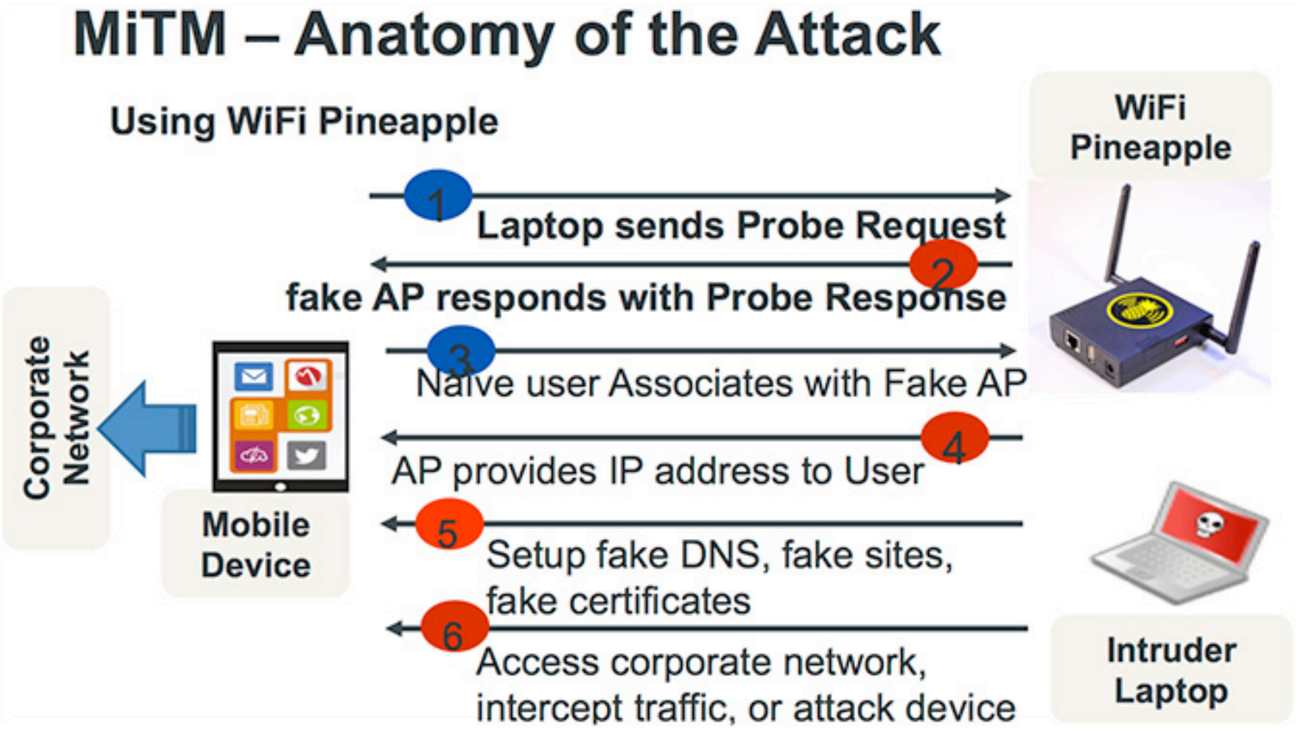
Content

Deauth/Disassociate Packet

SSID = CoffeeShop

- Intruder sets up a fake WiFi Access Point with same SSID & Internet Access to sit in the path of the connectivity
- Goal: Launchpad for attacks on mobile device or the resource it's connecting too (email, intranet site, etc.)

These tools also allow the attacker to set up a fake server-side certificate, spoof DNS, and ultimately redirect users' connections to a fake server. When the user connects, the connection can be terminated at the fake server, thus allowing the traffic to be decrypted (for example with SSLStrip) and sensitive data to be revealed.



MiTM – Anatomy of the Attack

Using WiFi Pineapple

WiFi Pineapple

1 Laptop sends Probe Request

2 fake AP responds with Probe Response

3 Naïve user Associates with Fake AP

4 AP provides IP address to User

5 Setup fake DNS, fake sites, fake certificates

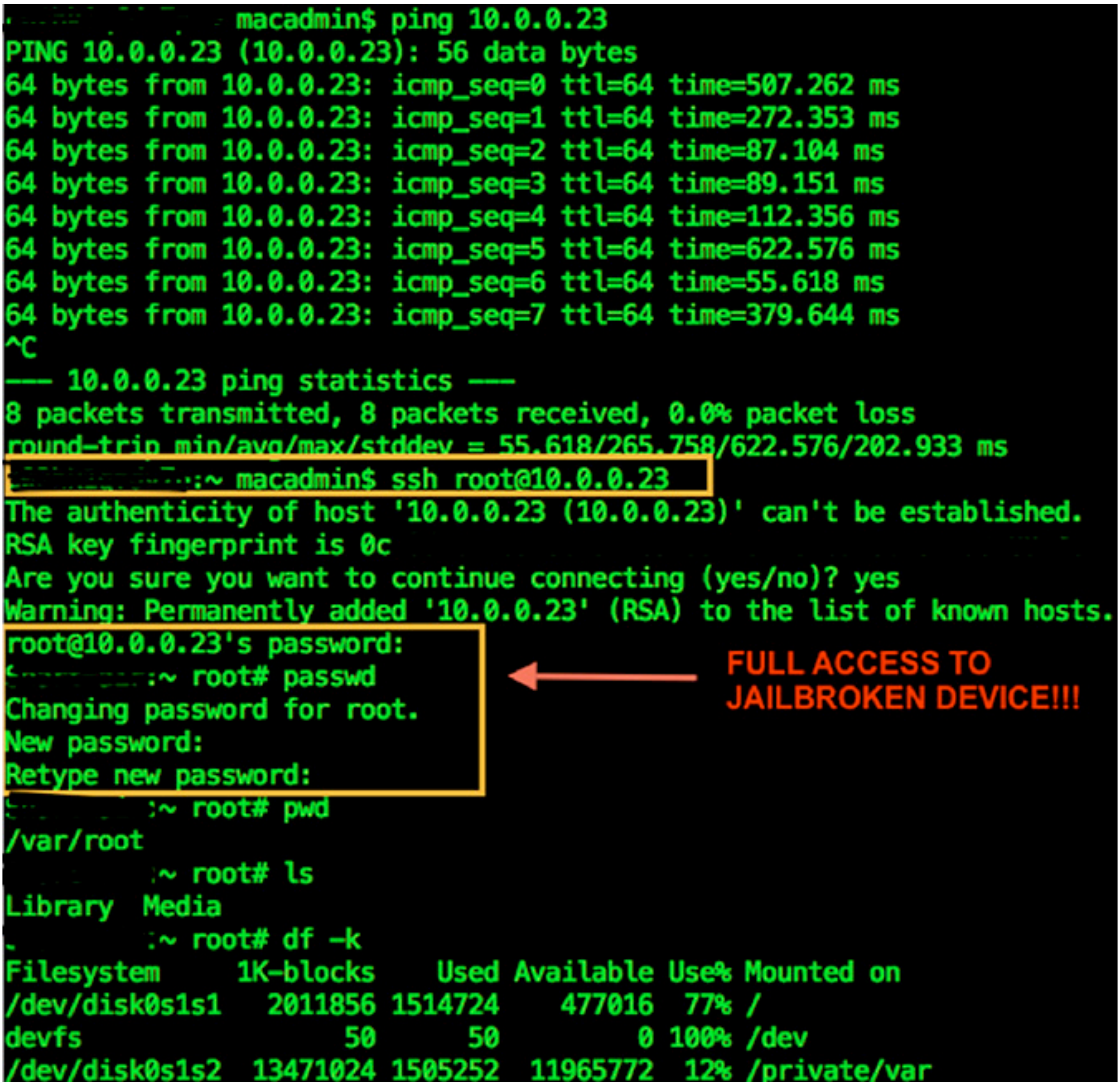
6 Access corporate network, intercept traffic, or attack device

Corporate Network

Mobile Device

Intruder Laptop

The attacker can also attempt to target the user's device directly. Some users like to jailbreak or root their devices to unlock additional features, or load custom ROMs. Of course jailbreaking or rooting a devices breaks the application sandboxing built into the mobile operating system, thus exposing it to malware threats. What many users don't realize is that it may also expose them on the network! For example, when you jailbreak an iOS device it can then be accessed over the network. Hackers know this, and will attempt to login to the iOS device using the default username ("root") and password ("alpine"). Once logged in, the attacker can obviously access sensitive information.



```
[redacted] macadmin$ ping 10.0.0.23
PING 10.0.0.23 (10.0.0.23): 56 data bytes
64 bytes from 10.0.0.23: icmp_seq=0 ttl=64 time=507.262 ms
64 bytes from 10.0.0.23: icmp_seq=1 ttl=64 time=272.353 ms
64 bytes from 10.0.0.23: icmp_seq=2 ttl=64 time=87.104 ms
64 bytes from 10.0.0.23: icmp_seq=3 ttl=64 time=89.151 ms
64 bytes from 10.0.0.23: icmp_seq=4 ttl=64 time=112.356 ms
64 bytes from 10.0.0.23: icmp_seq=5 ttl=64 time=622.576 ms
64 bytes from 10.0.0.23: icmp_seq=6 ttl=64 time=55.618 ms
64 bytes from 10.0.0.23: icmp_seq=7 ttl=64 time=379.644 ms
^C
--- 10.0.0.23 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 55.618/265.758/622.576/202.933 ms
[redacted]:~ macadmin$ ssh root@10.0.0.23
The authenticity of host '10.0.0.23 (10.0.0.23)' can't be established.
RSA key fingerprint is 0c [redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.23' (RSA) to the list of known hosts.
root@10.0.0.23's password:
[redacted]:~ root# passwd
Changing password for root.
New password:
Retype new password:
[redacted]:~ root# pwd
/var/root
[redacted]:~ root# ls
Library  Media
[redacted]:~ root# df -k
Filesystem     1K-blocks    Used Available Use% Mounted on
/dev/disk0s1s1   2011856 1514724    477016  77% /
devfs                 50      50         0 100% /dev
/dev/disk0s1s2  13471024 1505252  11965772  12% /private/var
```

FULL ACCESS TO JAILBROKEN DEVICE!!!

Certificates prevent messiness

So what can an enterprise administrator do to protect users from these network attacks when they are not on the administrator's network? There are several countermeasures they can employ exist in mobile to protect users from these attacks, and most importantly protect corporate data.

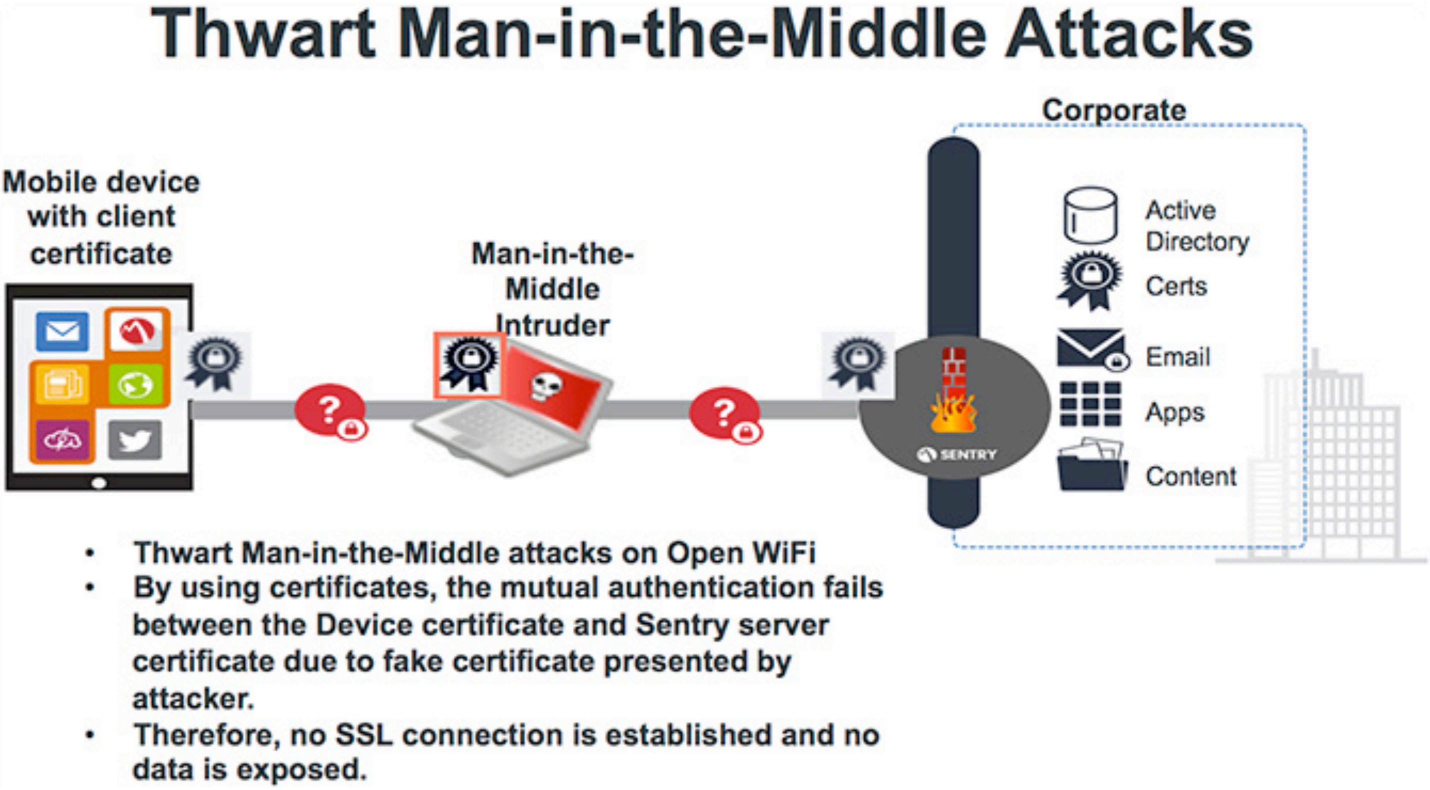
One of the approaches involves embracing a technology that's been around for many years: digital certificates. Enterprise folks have different opinions about certificates stemming from the PC era. Mobile devices have changed that mentality because these devices are built from the ground up with support for certificates. Certificates are easy to deploy to mobile devices through the use of an MDM/EMM product. Certificates can be automatically generated and deployed to the device with a profile pushed by the MDM/EMM solution.

This can allow certificates to be used for authentication to resources such as email, SharePoint, file shares, apps, web resources, and more. And if you have password reset policies and challenges with users calling the helpdesk, this approach can eliminate those issues as well.

Keeping with the theme of this article, they also do a great job of mitigating Man-in-the-Middle and interception attacks, by leveraging a feature built into the SSL/TLS protocol referred to as "mutual authentication".

The server-side cert and client certificates pushed to the device are used to mutually authenticate before data is transmitted.

Here's an example: when users unknowingly connect to a malicious open WiFi or open WiFi with a malicious user, their client certificate is presented to the other endpoint. This could be a VPN endpoint, or a per-app VPN endpoint on a service-by-service basis. If the user connects to their ActiveSync email, the certificate is presented and validated on the server, and vice versa. If the handshake is successful, the connection is allowed and data is transmitted allowing users to check their email. If the handshake fails, it's an indication that the client certificate can't validate the server side certificate, and no data is transmitted or exposed.



Thwart Man-in-the-Middle Attacks

Mobile device with client certificate
Man-in-the-Middle Intruder
Corporate
SENTRY
Active Directory
Certs
Email
Apps
Content

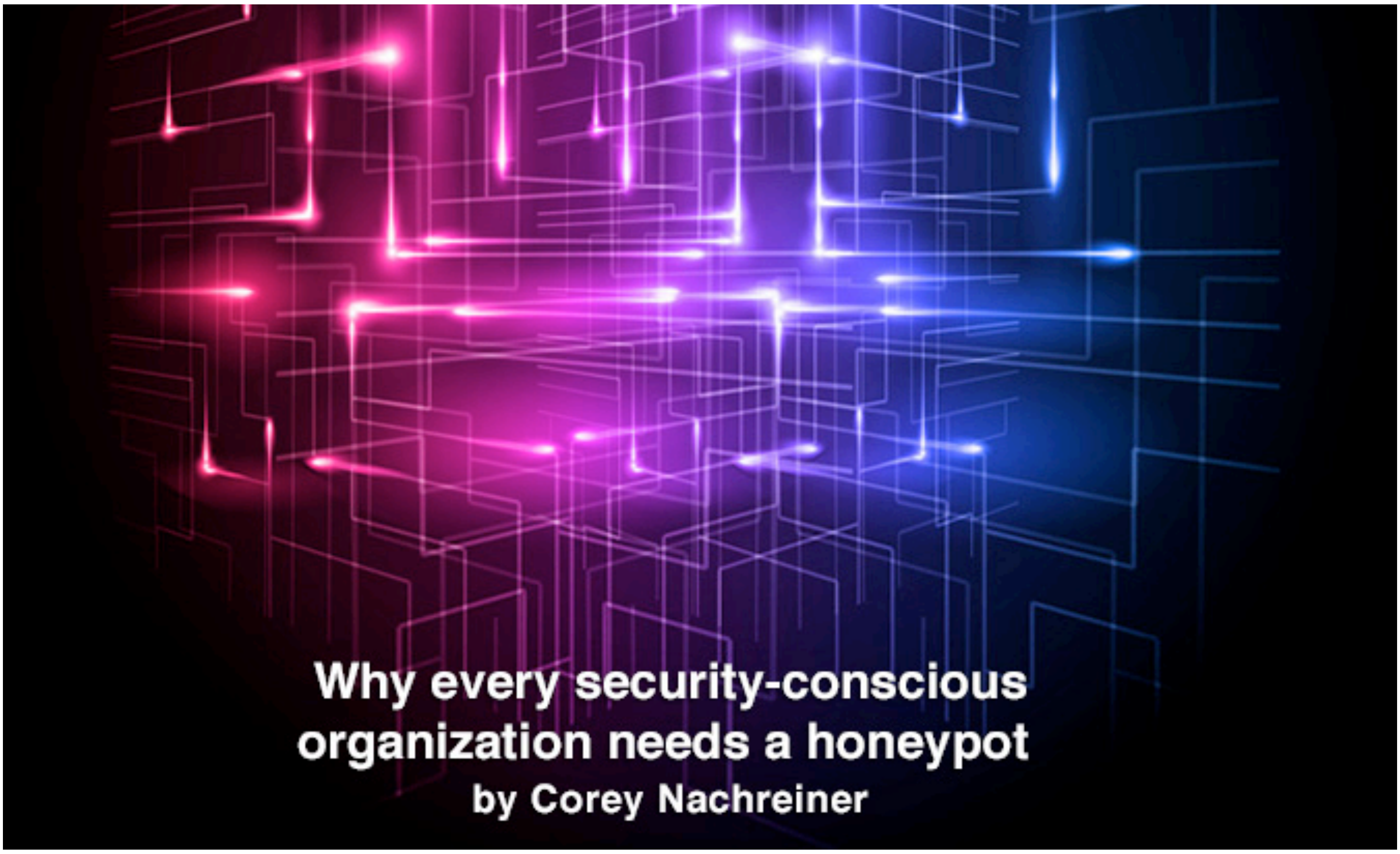
- Thwart Man-in-the-Middle attacks on Open WiFi
- By using certificates, the mutual authentication fails between the Device certificate and Sentry server certificate due to fake certificate presented by attacker.
- Therefore, no SSL connection is established and no data is exposed.

This addresses the interception and MitM network attacks, but what about the direct attacks on the end-users' device? As we mentioned, the single largest threat are those corporate devices that are jailbroken or rooted. Your MDM/EMM solution should provide for jailbreak and root detection combined with some form of a quarantine to remove corporate data from the device to mitigate exposures of sensitive enterprise data.

Network attacks can be broad and extensive, but the countermeasures for mobile devices do not need to be sophisticated to mitigate those threats. Leveraging client certificates with mutual authentication and a solid MDM/EMM solution can provide a great baseline for protecting your enterprise data-in-motion and data-at-rest on the devices.

While it's clear that IT has plenty to worry about when it comes to guarding users' mobile apps, content and devices, solutions that can get the job done already exist. Even though choice is messy, it's also necessary to enable the productivity and efficiency gains that are driving mobility in the first place.

Mike Raggo (CISSP, NSA-IAM, CCSI, ACE, CSI) is the Security Evangelist at MobileIron (www.mobileiron.com). He applies over 20 years of security technology experience and evangelism to the technical delivery of mobile security solutions. Mike's technology experience includes mobile device security, penetration testing, wireless security assessments, compliance assessments, incident response and forensics, security research. In addition, Mike conducts ongoing, independent research on various data hiding techniques including steganography, Wireless and Mobile Device attack, and countermeasure techniques.



Why every security-conscious organization needs a honeypot

by Corey Nachreiner

In the mid 1900s, a guy named John Haldane figured out that birds die pretty quickly when poisoned by carbon monoxide, after which coal miners started using them as early warning systems for toxic gas. We need the same for computer security. No defense is infallible, so organizations need digital canaries to warn them about poisoned networks.

When you think about the layers of security your business needs, you probably think about firewalls, authentication systems, intrusion prevention, antivirus, and other common security controls. However, I suspect few think about honeypots. That's a shame, as honeypots make perfect network security canaries, and can improve any organization's defense.

As an infosec professional, you've probably heard of a honeypot—a digital trap set to catch computer attacks in action. In essence, honeypots are systems that mimic resources that might entice an attacker, while in reality they're fake systems designed to contain and monitor attacks. In the same vein, a honeynet is just a collection of different honeypots.

There are many different varieties of honeypots, each designed to recognize and observe diverse types of attacks. Some catch network attacks (Honeyd), others catch web application attacks (Glastopf), and some are designed to collect and observe malware (Dionaea). You can check out The Honeynet Project (www.honeynet.org) for a fairly complete list of different kinds of honeypots.

These different honeypots also have varying levels of depth. For instance, a low-interaction honeypot might just emulate basic network services, perhaps only presenting a service banner and command prompt, but not offering much interaction to potential attackers (making them easier for attackers to detect).

Whereas, high-interaction honeypots can imitate full server systems, tricking hackers into carrying out their attacks further, allowing you to analyze them in depth.

With all the different varieties to choose from, each with varying levels of capability, honeypots might sound a little over complicated and perhaps too cumbersome for a small organization. In fact, some of the research-focused ones are certainly overkill for anyone but security academics. However, you don't need the most complex feature-packed honeypot for your simple purpose.

A production honeypot is a relatively low maintenance system, primarily used to detect attacks (rather than fully emulate and analyze them). Production honeypots make great network canaries. Over the years, production honeypots have evolved and become much easier for the average Joe to deploy. While most honeypots began as command line Linux packages, requiring manual installation and configuration, new solutions have surfaced making these packages more user-friendly, even for Linux newbies.

For instance, lately a number of Live CD distributions have come out specifically made for honeypots and honeynets. Rather than having to install a Linux distribution (distro) from scratch, and configuring everything yourself, these live honeypot distros have everything set up and ready to go. All you have to do is boot from a USB key or spin-up a virtual machine. Best of all, these honeypot distros are free. Three great examples include: HoneyDrive, Active Defense Harbinger Distribution (ADHD) and Stratagem.

If the convenience of live honeypot distros wasn't enough, newer honeynet projects have also made the older command line tools much easier to use. For instance, Project Nova adds a GUI, and many additional capabilities, to the trusty and popular Honeyd project. Nova makes Honeyd much more approachable to the average IT guy, making it dead simple for you to deploy a simple production honeynet in even the smallest organization. Better yet, Nova comes preinstalled in distros like ADHD, so all you have to do is boot ADHD, start Nova, and you are ready to experiment.

With all these easy and free options, there's little excuse not to at least try a honeypot. I suggest starting with the combination I mentioned above. Use the ADHD ISO to create either a bootable USB drive or virtual machine, spin it up, and give Nova a try. When you first boot ADHD, you'll see a "Usage documentation" link on your desktop. Double-clicking it will bring up a file that shares all the information you need to know to get started with some of the honeypot packages, including Nova. Or just refer to this guide on how to get Nova started.

If you run Nova with its default settings, it sets up three fake honeypot machines—a Linux server, Windows Server, and BSD Server—and it monitors them for network connections.

These basic honeypots act like those canaries in coal mines, warning you of dangerous activity. If Nova sees unusual connections to these machines, you know someone might be snooping around your network. Nova will also monitor for other types of attack traffic too, and warn you when it finds any IP addresses that act suspiciously.

Once you set up this simple honeynet, all you have to do is occasionally monitor it for unusual activity. However, after seeing what this simple setup can do, you might find you're intrigued by the capabilities of honeypots. If so, there's a lot you can explore in ADHD and Nova. For example, rather than sticking with Nova's default setup, you can add a bunch of fake nodes that emulate your actual server setup.

You can also explore the other types of honeypots ADHD provides, such the web application honeypot, Weblabyrinth, or file system honeypots like Artillery.

Whether or not you explore all the available honeypots is up to you, but you really should consider installing at least a basic one. All the big public data breaches over the past few years have shown us that we'll never have impermeable defenses.

No matter how many walls you build around your information, attackers will find weakness, and you data will leak out. That's why honeypots can play a crucial role in your organization's security strategy as the digital canary warning you before impending disaster.

Corey Nachreiner is the Director of Security Strategy and Research at WatchGuard Technologies (www.watchguard.com). Corey speaks internationally and is often quoted by other online sources. Corey enjoys "modding" any technical gizmo he can get his hands on, and considers himself a hacker in the old sense of the word.

acunetix

Are hackers finding their way into your business?

70% of networks and websites are hackable!
Check for open holes before hackers get in.

Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases. Firewalls, SSL and locked-down servers are futile against web application hacking.

Audit Your Website Security with Acunetix Vulnerability Scanner

Acunetix is available Online (OVS) and on Premise (WVS):

- ✓ Automatically checks web applications for XSS (Cross Site Scripting), SQL Injection & other vulnerabilities.
- ✓ Checks for known vulnerabilities in popular web applications such as Joomla, PHPbb.
- ✓ Quicker Remediation with the Innovative AcuSensor Technology
- ✓ Full HTML5 Support with Acunetix DeepScan
- ✓ Scans Password Protected Areas Automatically
- ✓ Comprehensive Reports for Legal and Regulatory Compliance
- ✓ Free Network Scanning of Perimeter Servers

Register Online or Download today

acunetix

REACH US ON
info@acunetix.com

(+1) 404 9903280
(+44) (0) 330 202 0190

www.acunetix.com

Securing the U.S. electrical grid

with Dan Mahaffee, the Director of Policy at CSPC

Interview by Mirko Zorz

The Center for the Study of the Presidency & Congress (CSPC) launched a project to bring together representatives from the Executive Branch, Congress, and the private sector to discuss how to better secure the U.S. electric grid from the threats of cyberattack, physical attack, electromagnetic pulse, and inclement weather. The result is the "Securing the U.S. Electrical Grid" report, and talking about critical security challenges we have Dan Mahaffee, the Director of Policy at CSPC.

How can politics influence the rise of critical infrastructure security on a national level?

Politics will certainly play a role in how our nation approaches critical infrastructure security. Many of the current bureaucratic structures for critical infrastructure security have arisen from politics. The Department of Homeland Security reports to over 100 committees and subcommittees because of politics.

One ongoing political debate is how to organize the various government agencies and entities responsible for cybersecurity—political influence and budget dollars are at stake. Given the importance of communication between government and critical infrastructure, it is important to provide some level of stability in the relationship between government and private sector operators.

Instead of reorganization, political leaders should emphasize clearer divisions of existing authority and streamlined communication within government regarding grid issues.

Additionally, cybersecurity legislation—along with most legislative business—has fallen victim to a deadlocked Congress. Even though it seems that the House and Senate have agreed on 90% of the legislation, politics has prevented the bills from going to a conference committee where the remaining 10% could be resolved. This political environment is even more difficult following the Snowden leaks, and it will require political leadership—both from elected officials and industry leaders and advocacy groups—to explain the importance of critical infrastructure protection to the American people and to seek the compromises to pass needed legislation.

Should the USA allow foreign companies to produce software/hardware for the domestic smart grid? How can these solutions be tested in order to prevent accidental or intentional failures?

In a globalized world, the issue of supply chain security is an area of significant concern. In some major countries there is a far blurrier line between government and the private sector when it comes to technology companies, and the United States needs to be aware of the security risks posed by these companies' hardware and software. U.S. policymakers have demonstrated their leadership on this issue, but there are still concerns about how software or various components of hardware might introduce vulnerabilities to U.S. infrastructure.

However, in a globalized world, we also cannot afford to succumb to the temptations of protectionism or risk retaliation against the operations of U.S. technology companies doing business overseas.

A combination of government and private sector testing processes can be implemented to test hardware and software for counterfeit components, potential backdoors, or other vulnerabilities, and these processes can be applied to both imported and domestically produced systems.

Additionally this testing can avoid a one-size-fits-all approach by evaluating not only the security of the product but also the criticality of its intended destination. Obviously hardware or software that will be installed at key grid nodes, links to other critical infrastructure, or major civil or military facilities will undergo more rigorous testing than less critical sites.

Through the buying power of the government and major utilities, manufacturers could be incentivized to meet these testing and specification requirements across their product lines.

Manufacturers will likely seek to differentiate their products by demonstrating that their products meet these standards. In a way, this could be similar to the "UL" logo, the "Good Housekeeping Seal of Approval," or the "MIL-SPEC" designation that graces many other products.

A combination of government and private sector testing processes can be implemented to test hardware and software for counterfeit components, potential backdoors, or other vulnerabilities, and these processes can be applied to both imported and domestically produced systems.

As we move closer to a world where almost every device is going to be connected to the Internet, how can we mitigate the onslaught of entirely new threats while we're not able to fend off even the oldest of attacks?

During our project, we often heard it described as the challenge of the grid moving from the "Edison Era to the Google Era." Policies should seek to facilitate tools that use this increased connectivity to provide immediate analysis of grid use and network traffic. The participants in our discussions indicated that the most fundamental tool to address attacks—old and new—is some form of information sharing mechanism with liability protections.

Such a tool—only available through Congressional legislation—can address today's security challenges and facilitate current and future technologies that allow for real time, machine-to-machine cyber threat information sharing and rapid incident response.

Additionally, as an increasing array of systems and appliances are connected to the grid, both government and the private sector should facilitate lines of communication between utility companies and the wide array of manufacturers developing control systems, appliances, cars, and other consumer products that will be connected to the grid. One current example is the work already underway at various national laboratories to explore the integration of electric cars into grid systems. Smart policies will seek to facilitate an ongoing security discussion and vulnerability testing rather than a static benchmark that will be quickly surpassed by technological advances.

Many information security professionals would argue that the key to an organization's security is security awareness, as it's usually the weakest link that enables cyber attackers to execute an efficient attack. How can we motivate an entire nation to educate themselves and understand the risks? It looks like a massive challenge that will have to pull together the resources from both the government and the private sector. How can the CSPC help in this regard?

As your question indicates, the human factor is one of the most important—if not the most important—aspects of physical and cyber security. Security awareness needs to be both top-down and bottom-up in an organization. While this is true of any organization, it is vital in a critical infrastructure provider.

At the top, security awareness requires constant communication between CEOs, CFOs, and COOs and their CSOs and CISOs.

Beyond the C-suites, every employee and vendor must also be aware of how their decisions may affect the security of a company. As social engineering becomes a key method for cyber attackers, individuals will need to be increasingly cognizant of how threat actors can pose as colleagues, vendors, social networks, or other legitimate activities.

This is indeed a massive challenge that will require resources from the government and private sector, but similar challenges have been overcome in the past. CSPC is an organization that looks at the lessons of history and facilitates opportunities for dialogue between the White House and Congress and between the government and the private sector.

CSPC is in a unique position to understand how combining historical lessons in public awareness campaigns—pollution and smoking are ones that immediately come to mind—with continued communication between our government and private sector leaders can improve cybersecurity.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

> Visit www.insecuremag.com
> SUBSCRIBE TO (IN)SECURE MAGAZINE

OS X version of Windows backdoor spotted

The XSLCmd backdoor for OS X was first spotted when it was submitted to VirusTotal on August 10, 2014, and not one of the AV solutions it uses detected it as malicious. Subsequent analysis by FireEye's researchers showed that the malware's code is based on that of its homonymous Windows counterpart that was first seen used in 2009, and has been used widely and extensively in the last couple of years.

"Its capabilities include a reverse shell, file listings and transfers, installation of additional executables, and an updatable configuration," the researchers noted. "The OS X version of XSLCmd includes two additional features not found in the Windows variants we have studied in depth: key logging and screen capturing."

Going through the malware's code, the researchers had the impression that the rewriting and adding to the original code was done by another coder. Other changes they noted make them think that the OS X backdoor was created when OS X 10.8 was the latest, or the most common version of the OS in use, and that the coder made efforts to make the backdoor compatible with older OS X versions.

The group they believe is using the backdoor has been named by the researchers GREF, because it uses a number of Google references in their activities. Even though they have been known to use phishing emails to saddle targets with malware, GREF is one of the pioneers of the "watering hole" type of attacks. Back in 2010, the group also used a lot of 0-day exploits to compromise web servers to gain entry to targeted organizations, as well as to turn sites into "watering holes." And another thing to note is that they have never been too worried about masking their attacks.

"They are known to utilize open-source tools such as SQLMap to perform SQL injection, but their most obvious tool of choice is the web vulnerability scanner Acunetix, which leaves tell-tale request patterns in web server logs. They have been known to leverage vulnerabilities in ColdFusion, Tomcat, JBoss, FCKEditor, and other web applications to gain access to servers, and then they will commonly deploy a variety of web shells relevant to the web application software running on the server to access and control the system."

Researchers unlock TorrentLocker encryption

A team of Finnish researchers has discovered that the files encrypted by the recently unearthed TorrentLocker ransomware can be decrypted without paying the ransom - if the user has at least one of the encrypted files backed up somewhere, and that file is over 2MB in size.

Crediting Trend Micro reseachers with the discovery that the TorrentLocker "encrypted files by combining a keystream to the file with exclusive or (XOR) operation," researchers Taneli Kaivola, Patrik Nisén and Antti Nuopponen discovered that the malware contains AES code, and SHA256 and SHA512 hash algorithms.

"Exact details on how the encryption is done still remain unknown, but it strongly appears that the encryption is done with a stream cipher that is built using AES and hash functions. The fact that the keystream consists of 16 byte blocks also supports the assumption that AES is used to produce the keystream," they pointed out. The malware authors' mistake is the following: the malware uses the same keystream to encrypt all the files within the same infection.

"As the encryption was done by combining the keystream with the plaintext file using the XOR operation, we were able to recover the keystream used to encrypt those files by simply applying XOR between the encrypted file and the plaintext file," they shared. "Further analysis of the encrypted files also revealed that the malware program added 264 bytes of extra data to the end of each encrypted file, and that it only encrypts the first 2MB of the file, leaving the rest intact."

"The exact purpose of the extra 264 bytes that the malware program adds at the end of each file is still unknown, but it seems to be unique for each infection. As it is unique, it allowed us to write a software program that automatically recognizes which keystream has been used to encrypt the files," they concluded, and invited affected users to get in touch.

Salesforce users hit with malware-based targeted attack

Cloud-based CRM provider Salesforce has sent out a warning to its account administrators about its customers being targeted by the Dyreza malware.

"On September 3, 2014, one of our security partners identified that the Dyre malware (also known as Dyreza), which typically targets customers of large, well-known financial institutions, may now also target some Salesforce users," the alert said. "We currently have no evidence that any of our customers have been impacted by this, and we are continuing our investigation. If we determine that a customer has been impacted by this malware, we will reach out to them with next steps and further guidance."

Dyreza is a whole new banking trojan family, which was first spotted earlier this year targeting customers of US and UK banks.

"The code is designed to work similar to ZeuS and as most online banking threats it supports browser hooking for Internet Explorer, Chrome and Firefox and harvests data at any point an infected user connects to the targets specified in the malware," CSIS researcher Peter Kruse shared at the time.

The malware effectively performs a Man-in-the-Middle attack and, in this case, intercepts the information submitted by users - username, password, and even their two-factor authentication token - by redirecting them to a spoofed Salesforce login page. The company does not mention how the malware infects the targets' computer, but if past approaches are any indication, users are targeted with phishing emails carrying or linking to the malware, which masquerades as a legitimate application.

Over 1,000 businesses compromised with Backoff malware

The US Department of Homeland Security has repeated a warning to businesses about the Backoff malware.

"The DHS encourages organizations, regardless of size, to proactively check for possible Point of Sale (PoS) malware infections," the advisory states.

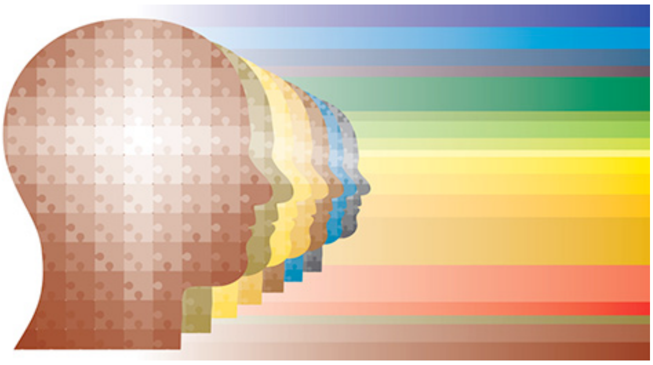
"One particular family of malware, which was detected in October 2013 and was not recognized by antivirus software solutions until August 2014, has likely infected many victims who are unaware that they have been compromised."

The initial advisory went out on July 31, 2014, and detailed the effects of the malware. In this latest one the DHS noted that the Secret Service has already responded to network intrusions at numerous businesses throughout the United States, and that seven PoS system providers/vendors have confirmed that they have been hit.

Apparently, the estimate is that over 1,000 US businesses have been affected, and the DHS is advising organizations to contact their IT team, antivirus vendor, managed service provider, and/or point of sale system vendor to check for intrusions or possible vulnerabilities that could lead to one.

If they find that they have become a victim of this malware, they are advised to contact their local Secret Service field office.

Tool restores SynoLocker-encrypted files



Security company F-Secure has created a tool that could help SynoLocker victims get their files back, but it only works if they have received - bought - the correct decryption key.

SynoLocker, as you might remember, is a piece of ransomware targeting users of Synology NAS devices. It encrypts the files contained on them and asks 0.6 Bitcoin for the decryption key.

Recently, there have been indication that the crooks behind the scheme might be ending it as they have been spotted trying to sell the remaining unclaimed keys in bulk.

F-Secure does not encourage users to pay the ransom in order to get the decryption key, but they know that some users will. But even that is not a guarantee that they will get their files back.

"In many of the cases we have observed, the decryption process didn't actually work or the decryption key provided by the criminals was incorrect," said F-Secure intern Artturi Lehtio.

In order to help that subset of users, the company has released a Python script that should decrypt the encrypted files.

"The tool does not in any way break the encryption of files created by SynoLocker and it does not attempt to bruteforce the decryption key. It will only work, if the decryption key is already known," he explained.

"Another use case for our decryption tool is a situation where a user has paid the ransom but can't use the decryption key as they have removed the SynoLocker malware from the infected device. Instead of reinfecting your device with the malware (which is a bad idea), you can use the key together with our script to decrypt your files."

Documentation Toolkit
ISO 27001
27001 Academy

Using Hollywood to improve your security program

by Dwayne Melancon

I spend a lot of time on airplanes, and end up watching a lot of movies. Some of my favorite movies are adventures, spy stuff, and cunning heist movies. Recently, I realized that a lot of these movies provide great lessons that we can apply to information security.

Lesson 1: Be paranoid about handoffs and blind spots

Many data breaches occur because attackers take advantage vulnerabilities in the “spaces between” different functions. They exploit these weaknesses, often during a handoff from one silo to another.

For example, there are a lot of movies in which criminals take advantage of short-term blind spots to do a “switcheroo.” In a lot of heist movies, a truck goes into a tunnel filled with gold but when it exits at the other end of the tunnel the criminals have swapped it for an identical truck filled with something worthless.

The lesson here is “trust, but verify.” Try to instrument as much of your process as possible to minimize blind spots and, when something (a system, a transaction, an install package, etc.) is out of your control for some period of time, validate it before you assume it hasn’t been tampered with.

Lesson 2: Use baselines of what’s normal, so you can quickly detect the abnormal

[Spoiler alert!] In the movie “The Inside Man,” the police spend a lot of time trying to figure out how criminals got something valuable out of the bank, but are never able to figure it out. In reality, the “stolen” item had never left the bank at all – the criminals had added a false wall in the vault, and one of the criminals was in the resulting hollow space with some food, water, and a bunch of diamonds. He waited a while for the frenzy to die down, left his crawl space, and simply walked out of the bank

unnoticed. This technique worked because nobody noticed that the vault room was slightly smaller than it had been in the past.

From this movie, we can learn to rely on baselines and automation to catalog the normal and expected state of things, so we aren't fooled by the equivalent of a false wall in your infrastructure. Cyber criminals can hide things in plain sight by tucking them away inside an alternate data stream that is invisible to your normal file management tools. Take steps so you aren't fooled by innocuous appearances. Use file hashes, transaction checksums and signed components to ensure that even subtle changes are brought to your attention.

Lesson 3: Beware of distractions, impostors, spoofed information, and sleight of hand

Lesson 3 is really a bunch of lessons all rolled into one, but I loved the movie so bear with me (and yes, this is another *Spoiler Alert*).

In the 2001 movie "Ocean's Eleven," Danny Ocean (George Clooney) and his crew are able to rob a casino, right under the owner's nose. A number of attacks are involved:

• In various parts of the movie, criminals pose as consultants, employees, and other experts to gain access to the inner workings of the casino. This is analogous to credential theft or a compromise of your trusted insiders.

• The surveillance system is compromised to make the casino operators believe everything is normal. Ocean's crew tamper with the video feed so the casino ends up watching fake camera footage instead of what's really happening. This is the equivalent of cyber criminals tampering with logs and other traces to cover their tracks.

• There are also several instances in which the casino owner and law enforcement personnel are fed bogus information that sends them on wild good chases with the goal of luring them away from the location where the real crime was occurring. We've seen DDOS attacks, cyber vandalism, and other tactics in the infosec world used in a similar way to distract organizations from the real attack (often fraud, or data exfiltration in some other area of the business).

In these examples, we can implement safeguards such as multifactor authentication, strong identity and access management, oversight and "big picture" continuous monitoring. These approaches reduce the risk that we will miss criminal acts because we're distracted by a theatrical event designed to grab our attention, tie up our resources and lure us away from the real crime.

Thinking like Hollywood is a fun and useful way to find weaknesses in your security posture.

Think like Hollywood

These examples provide mental models that can help us think about information security in a different way. If your data security strategy were featured in a Hollywood blockbuster, how would you be fooled? Where are the weak spots that criminals could take advantage to get at your company's "crown jewels?"

Thinking like Hollywood is a fun and useful way to find weaknesses in your security posture. I think you'll find that most of the opportunities for improvement center around weak or sloppy handoffs; the lack of a clear picture of what "normal" looks like; the inability to notice small changes in your environment; the tendency to trust without verifying; and a bias to focus on the biggest, latest, and loudest incident you encounter.

In Hollywood heist movies, the bad guys often win. In real life, you have the power to make sure they don't – imaging you're in a Hollywood movie can help, and it's a lot more fun than a pen test.

Dwayne Melancon is the CTO at Tripwire (www.tripwire.com). When he's not busy fighting cybercrime, he meets with as many customers as he can to foster a deep understanding of their problems, and collaborate with them on practical, real world solutions.

How a large ISP fights DDoS attacks with a custom solution

by Mirko Zorz

DDoS attacks are a growing problem. In July, Arbor Networks released global DDoS attack data derived from its ATLAS threat monitoring infrastructure that shows a surge in volumetric attacks in the first half of 2014 with over 100 attacks larger than 100GB/sec reported.

Sadly, it's not just the strength we should be worried about. In fact, BT found that DDoS attacks are becoming more effective, causing major disruption and sometimes bringing down organizations for entire working days.

We often hear about attacks against websites, most of which are mitigated by one of the many DDoS mitigation services available on the market. What I always wondered was how the big guys tackle these attacks. What weapons can an ISP bring to the battleground?

Technology made to fit

Sakura Internet, one of Japan's largest Internet Service Providers, developed a technology that ingests massive IP traffic flow data streams and performs in-memory analytics to identify and stop DDoS attacks on its network as they happen, while simultaneously enabling legitimate traffic to continue.

They built a DDoS attack mitigation solution on the high-speed NewSQL database VoltDB to have the capability to analyze 48,000 IP packets per second, allowing them to see in real time which sites are under attack, and perform source-and-destination-based filtering, allowing clean incoming packets to move through, while blocking the bad.

In April 2014, the very first month of the solution's production with VoltDB, Sakura detected and mitigated 60 DDoS attacks while also successfully restoring legitimate traffic to the majority of targeted sites - as the attacks were happening. Sakura was able to restore service in 49 of the 60 attempts it made, and in some cases, in as little as twenty seconds.

The man with the plan

The architect behind this solution is Tamihiro Yuzawa, a Network Engineer in charge of datacenter networking, inter-DC and inter-AS routing operations at Sakura Internet.

Yuzawa's team is in charge of Sakura's core network and his primary concern are large scale, bandwidth-hogging incoming DDoS attacks with junk packets that would not only disrupt legitimate communication to and from the victim host, but also cause collateral damage to other customers sharing their uplink with the attack target.

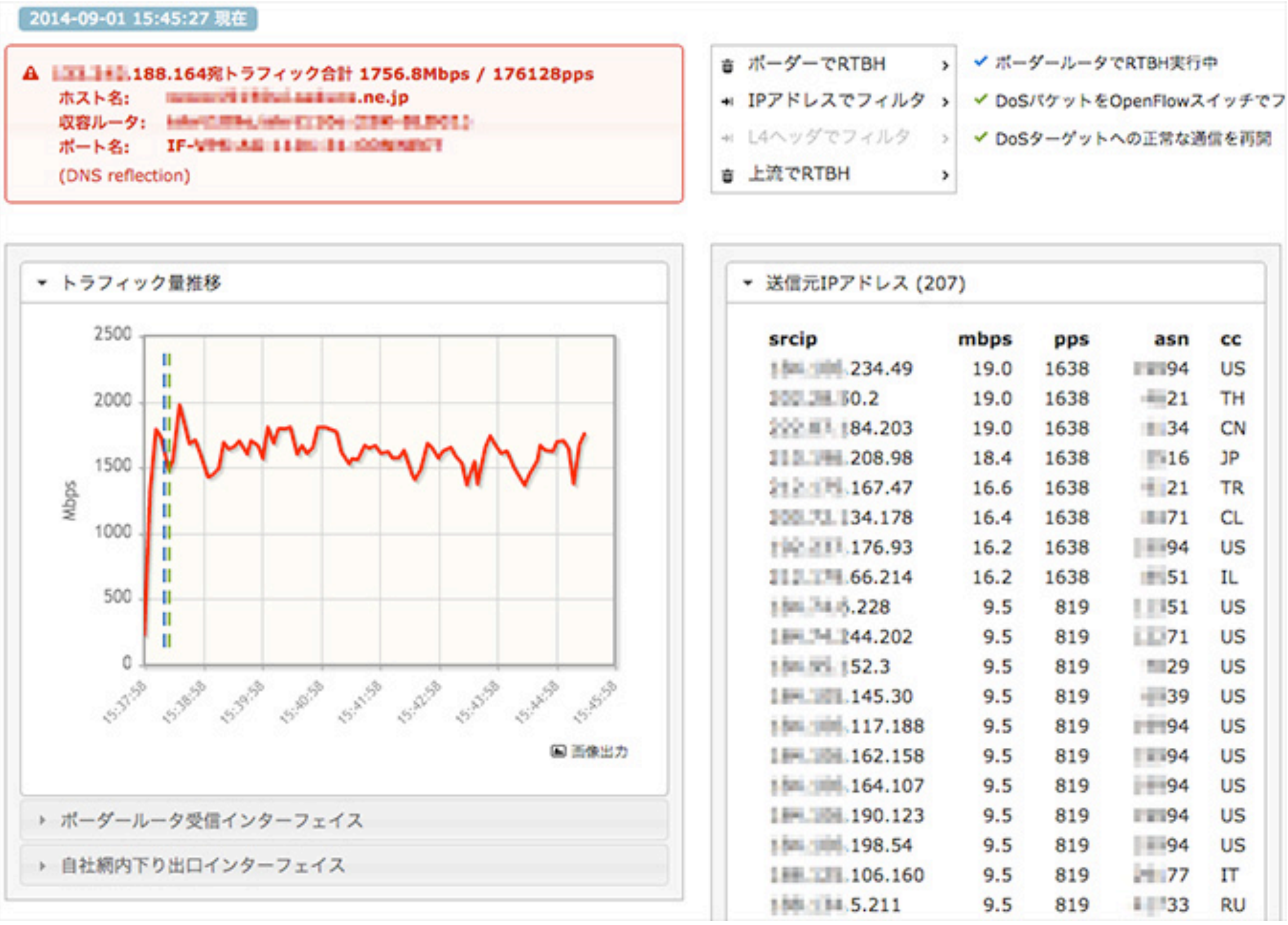
How damaging can DDoS be to an ISP? "If we fail to promptly mitigate an attack of the magnitude of 10Gbps or beyond, the consequence could be ugly route flaps in our network, which would seriously degrade our services," says Yuzawa.

In most cases, it takes less than 10 seconds for the attack traffic to grow over gigabits per second. Before they developed this solution, it was only after their network monitoring system would dispatch alerts for reachability problems that they would look into some other information to find out there had been a DDoS attack already coming in.

Yuzawa remembers that, back then, sampled traffic data was already available, with a couple of collectors up and running. But traditional RDBMSs would easily saturate and choke on a huge influx of sampled data, and were thus unable to execute queries for real-time analysis.

"We had been quite aware that it would take a truly fast data processing backend that would import and compute a massive amount of data without delay so as to detect an attack right away. That's why it jumped out at me when the release of VoltDB hit the news," Yuzawa said.

On the following page you can see a screenshot that showcases a part of the app's UI. To capture this image, Yuzawa used archived traffic sample data to replay a recent DDoS attack. Only the destination IP address (in red) has been masked with the test server's. While the attack continues at around 1.6~1.7Gbps, the blue line indicates the first step completed



2014-09-01 15:45:27 現在

⚠ [redacted].188.164宛トラフィック合計 1756.8Mbps / 176128pps
ホスト名: [redacted].ne.jp
収容ルータ: [redacted]
ポート名: IF-[redacted]
(DNS reflection)

✓ ボーダールータでRTBH実行中
✓ DoSパケットをOpenFlowスイッチでフ
✓ DoSターゲットへの正常な通信を再開

送信元IPアドレス (207)

srcip	mbps	pps	asn	cc
[redacted].234.49	19.0	1638	[redacted]94	US
[redacted]0.2	19.0	1638	[redacted]21	TH
[redacted]84.203	19.0	1638	[redacted]34	CN
[redacted].208.98	18.4	1638	[redacted]16	JP
[redacted].167.47	16.6	1638	[redacted]21	TR
[redacted]34.178	16.4	1638	[redacted]71	CL
[redacted].176.93	16.2	1638	[redacted]94	US
[redacted].66.214	16.2	1638	[redacted]51	IL
[redacted].228	9.5	819	[redacted]51	US
[redacted]44.202	9.5	819	[redacted]71	US
[redacted]52.3	9.5	819	[redacted]29	US
[redacted].145.30	9.5	819	[redacted]39	US
[redacted].117.188	9.5	819	[redacted]94	US
[redacted].162.158	9.5	819	[redacted]94	US
[redacted].164.107	9.5	819	[redacted]94	US
[redacted].190.123	9.5	819	[redacted]94	US
[redacted].198.54	9.5	819	[redacted]94	US
[redacted].106.160	9.5	819	[redacted]77	IT
[redacted].5.211	9.5	819	[redacted]33	RU

at 15:38:15, and the green line indicates the second step (cleaning) was activated at 15:38:23. And as of 15:45:27, 730 source IP addresses are being filtered.

There's a lot of talk about how Big Data can help mitigate DDoS attacks, but how does it work exactly? Yuzawa explains that every router deployed in their backbone network is capable of sampling packets as they arrive in the router's ingress interfaces, and encapsulating the sampled packets into a UDP message in a standardized format, which are then exported to the designated collector. The collector, acting as a database client, feeds the database with sampled traffic data as it arrives from the routers.

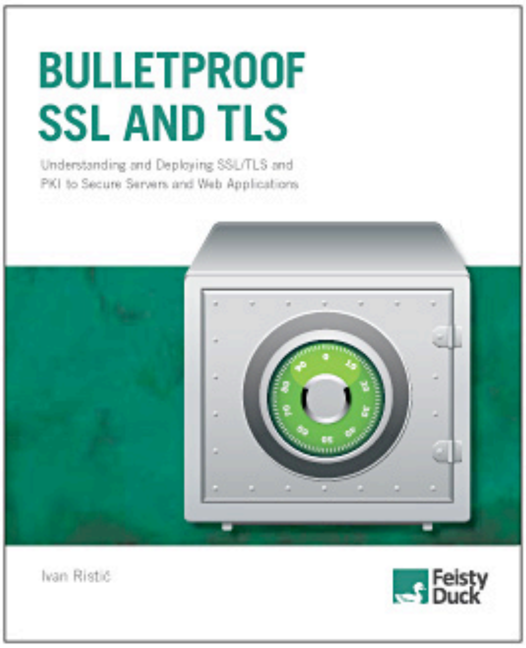
There are several other database client processes running all the time, one of which requests various types of aggregate queries per each destination IP address, so that it can identify a flow of malicious incoming traffic on the spot. Another client continues to profile each attack, including the origin IP addresses, also on the spot.

With the constantly updated information about each attack, the mitigation system protects legitimate traffic to the target host while blackholing attack packets.

When custom equals better

Yuzawa told me that over the years Sakura evaluated several commercial DDoS mitigation appliances, a couple of which showed impressive capabilities. However, in order to be able to execute truly effective countermeasures quickly, in the order of seconds, they needed to incorporate something very specific to their network design, configurations, and operations, and essentially create their own anti-DDoS solution.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org). He can be reached on Twitter as @helpnetsecurity.



BULLETPROOF SSL AND TLS
Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications
Ivan Ristić
Feisty Duck

This year's Black Hat USA featured more content than any previous year, including more than 180 speakers and researchers across 113 briefings, 10 timely roundtable sessions and a full day Kali Linux workshop – the most abounding lineup in the event's history. Content was king as Black Hat celebrated its seventeenth year in a new venue, Mandalay Bay. The Black Hat Review Board, made up of 23 of the security industry's most respected experts, reviewed more submissions this year than any year prior. In addition to the expansive Briefings schedule, other exciting events onsite broke the record books.

The Black Hat Arsenal returned for its fifth year, offering researchers and the open source community the ability to demonstrate live tools they develop and use in their daily professions.

The newly enhanced Black Hat Business Hall, the epicenter of where business happens at the show, this year featured 147 of the industry's top solution providers and start-ups showcasing the latest tools, technologies and services supporting the security community, which is a twelve percent increase from 2013. The Black Hat Executive Summit, an exclusive invitation-only gathering of more than 115 industry executives and security industry leaders, ignited open conversations and "think tank" style breakout sessions.

Black Hat USA 2014's keynote speaker was Dan Geer, Chief Information Security Officer at In-Q-Tel, and widely considered one of the security industry's foremost pioneers. In his talk, "Cybersecurity as Realpolitik," Geer examined the use of power in security and outlined a set of ideas and policy recommendations for the future of the industry. After the standing room only session, many attendees commented that this keynote presentation was one of the most impactful they'd seen.

Photos by (IN)SECURE Magazine and Black Hat.

The synergy of hackers and tools at the Black Hat Arsenal

by Mirko Zorz

Black Hat USA 2014 recently welcomed more than 9,000 of the most renowned security experts – from the brightest in academia to world-class researchers and leaders in the public and private sectors. Tucked away from the glamour of the vendor booths giving away t-shirts and the large presentation rooms filled with rockstar sessions, was the Arsenal - a place where developers were able to present their security tools and grow their community.

The Arsenal is the brainchild of NJ Ouchn, a well-known security expert and creator of ToolsWatch.org. His unrelenting passion for using freely-available tools during penetration testing engagements has evolved into what is really a conference within a conference and, for some, the main reason for coming to Las Vegas.

This year's Arsenal, which NJ managed with the help of Rachid Harrando, the CEO of NETpeas, hosted the authors of 54 tools coming from countries all over the world. To make things even more interesting, some of the tools were unveiled at the Arsenal and attendees had the opportunity to engage the developers immediately. There was something for everyone: from attacking VoIP, forensics to mobile hacking and beyond.

All the presenters I've talked to have nothing but praise for both NJ and the Arsenal. Dan Cornell, CTO at the Denim Group, told me that this is something he looks forward to every year because it is a great way to get his work in front of a critical audience of security experts.

"I've always been impressed with how well-run the event is – both with support from NJ as well as the Black Hat conference organizers. I enjoy the questions the most because they give us a great window into both new features we need to build as well as how we need to communicate about ThreadFix's (www.threadfix.org) current capabilities," Cornell said.

Georgia Weidman, CEO at Bulb Security, believes her Smartphone Pentest Framework (www.bulbsecurity.com/smartphone-pentest-framework) wouldn't have gotten any notice at all had it not been for the Arsenal. "Open source security tools are the backbone of security research these days, so having a place for them is a great service to the attendees of Black Hat as well as the writers of the tools," she said.

Bahtiyar Bircan, a security consultant and author of the Heybe Penetration Testing Automation Kit (github.com/heybe), said that the interaction with security practitioners at the Arsenal gave him new ideas and he encourages everyone to participate.

The Arsenal is essentially a breeding ground for cooperation and fresh ideas lacking corporate gimmicks. What routinely happens after the conference is that projects start to work together and integrate with each other, increasing their value exponentially, ultimatively increasing not only the value of the tools, but also elevating the profile of the developer. I've heard that a developer presenting this year was offered a full-time job right then and there.

Next time you're at Black Hat, make time for the Arsenal. It was the highlight of my week and I'm sure it will inspire you as well.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

Photos are a courtesy of Black Hat.

Web application security today
with Ferruh Mavituna, CEO at Netsparker

Interview by Mirko Zorz

Ferruh Mavituna is the CEO and Product Architect of Netsparker. In this interview he talks about his area of expertise - web application security.

Web application vendors are getting more responsive and are releasing security patches faster. Still, many problems remain. What are the most significant trends in web application security today?

Even though the industry is doing its best to raise web application security awareness, and more people in this business are now indeed more aware, unfortunately the only significant trend we are seeing is that more websites are getting hacked every day.

Most probably the source of the problem are the vendors themselves; they are operating in reactive mode rather than in proactive mode; they release patches when security issues are reported but they do not include web application security in their SDLC, hence they do not develop secure products in the first place to avoid the fiasco.

In all fairness though, each day more established businesses are investing in web application security, because they do understand how important it is, and what a negative impact a hack attack can have on their business. Yet there are many startups coming up, most of which have no security background or awareness at all. And once they have an online presence, they are a target and usually end up in the news.

So, how can we improve the situation? Even more awareness than there is already, more vendors should get involved in helping raising awareness and better incentives to help startups built secure web applications.

Based on your experience, what are the biggest misconceptions when it comes to security testing?

There are a number of misconceptions in the web application security industry, below are just the two most popular ones.

Hackers are not interested in hacking my website, I do not store sensitive information and my business is not popular: well said! It is true, maybe malicious hackers are not interested in your business, or your data, but what about the server resources and its bandwidth? Servers are not hacked just to steal sensitive data, but to serve as an automated bots, or to serve as a stepping stone for bigger attacks. The server's resources can be used to compute other attacks, or to store illegal material and redistribute it.

We manually audit our web applications, so they are secure: nothing against manual penetration tests. As a matter of fact I always recommend that an automated security scan should be accompanied by a manual audit. But manually auditing a modern web application is impossible.

A human is unable to check every potential attack entry point against hundreds of different vulnerability vectors and security issues. If you are manually testing your web applications you are wasting your precious time with something that can be automated.

What are the most important things to keep in mind when testing websites and web applications for security flaws?

First of all you shouldn't assume anything, 1 out of 200 SQL queries used in the application might be vulnerable, you cannot just assume they are all safe against SQL Injection attacks because the first 50 of them were. I have personally seen some crazy stuff in terms of development, so one should never assume anything while testing a web application.

Secondly, coverage is really important. Modern web applications have very big attack surfaces. Hitting all the code branches from a black-box perspective is quite challenging. You should find all the input places, not linked pages, backups, conditional branches, APIs, mobile interfaces, XML version of a JSON interface, etc.

Before calling it a day, you should ensure that you have that coverage, because attackers will attack to the weakest link, they won't try to bypass your authentication from the login form that has been tested 100 times, they will find that one obscure API call with limited checks.

There are tons of attackers out there and unlike you they don't have 5 man days scope to test your web application, but hundreds attackers with hundreds of man days available. They will find those rarely used features and exploit them, that's why one should ensure that the test coverage is complete.

A HUMAN IS UNABLE TO CHECK EVERY POTENTIAL ATTACK ENTRY POINT AGAINST HUNDREDS OF DIFFERENT VULNERABILITY VECTORS AND SECURITY ISSUES.

What is the impact of false positives in a web application security scan? How can they be mitigated?

False positives have a very negative impact on web application security and many people still do not comprehend the scale of the impact.

Starting with obvious, false positives are making web application security expensive and unaffordable for many businesses. For example during a typical penetration test, if the penetration tester expects the web application security scanner to generate false positives, he or she will dedicate an extra few days to verify the findings of the scanner. In business terms, an additional 2 or 3 days mean money.

If you hire a third party for penetration tests, an additional 2 or 3 days means thousands of dollars. Even if you have your own in-house security department; additional days to complete a penetration test means delaying the project, needing more man power and so on. Therefore even if you have your own in-house security department, false positives will increase the cost of penetration tests.

Apart from the cost, false positives also affect the outcome of a penetration test, and in most cases this leads to leaving vulnerabilities and other security holes open on your web applications, ready to be exploited by a malicious attacker.

For example if the automated web security scanner reports 100 SQL Injections and the penetration tester confirms that the first 50 are false positives it would be assumed that the other 50 are also false positives, hence risking of not addressing legitimate vulnerabilities.

This is not a matter of how dedicated the penetration tester is, this is a result of trying to keep the costs down and finishing the project as soon as possible due to pressures coming from the management or the customer.

And what if the penetration tester or the developer cannot replicate the scanner findings?

There are some vulnerability checks that can be very tricky to be verified manually and in some cases the penetration tester is not familiar with the vulnerability or the advanced bypass technique that the scanner employed. So in such cases, since automated scanners are unfortunately labeled with this false positive stigma, the tester would assume that the vulnerabilities he cannot replicate are false positives, and if some of them are legit they will never be addressed by the developers.

What can the industry do to mitigate this impact? The answer is simple: build better technology to ensure less false positives are reported. Of course, it is easier said than done. Though, there is light at the end of the tunnel.

When you look back at the statistics web vulnerability scanners are really improving in terms or reporting less false positives. Some others even go a step ahead and do automatically confirm the findings. How? By exploiting their own findings; if a vulnerability is exploited it is definitely not a false positive.

Cyber Security Expo 2014

www.cybersec-expo.com

ExCel London, UK / 8 October - 9 October 2014

HITBSecConf2014 - Malaysia: Past, Present & Future

conference.hitb.org

InterContinental Kuala Lumpur, Malaysia / 15 October - 16 October 2014

McAfee FOCUS 14

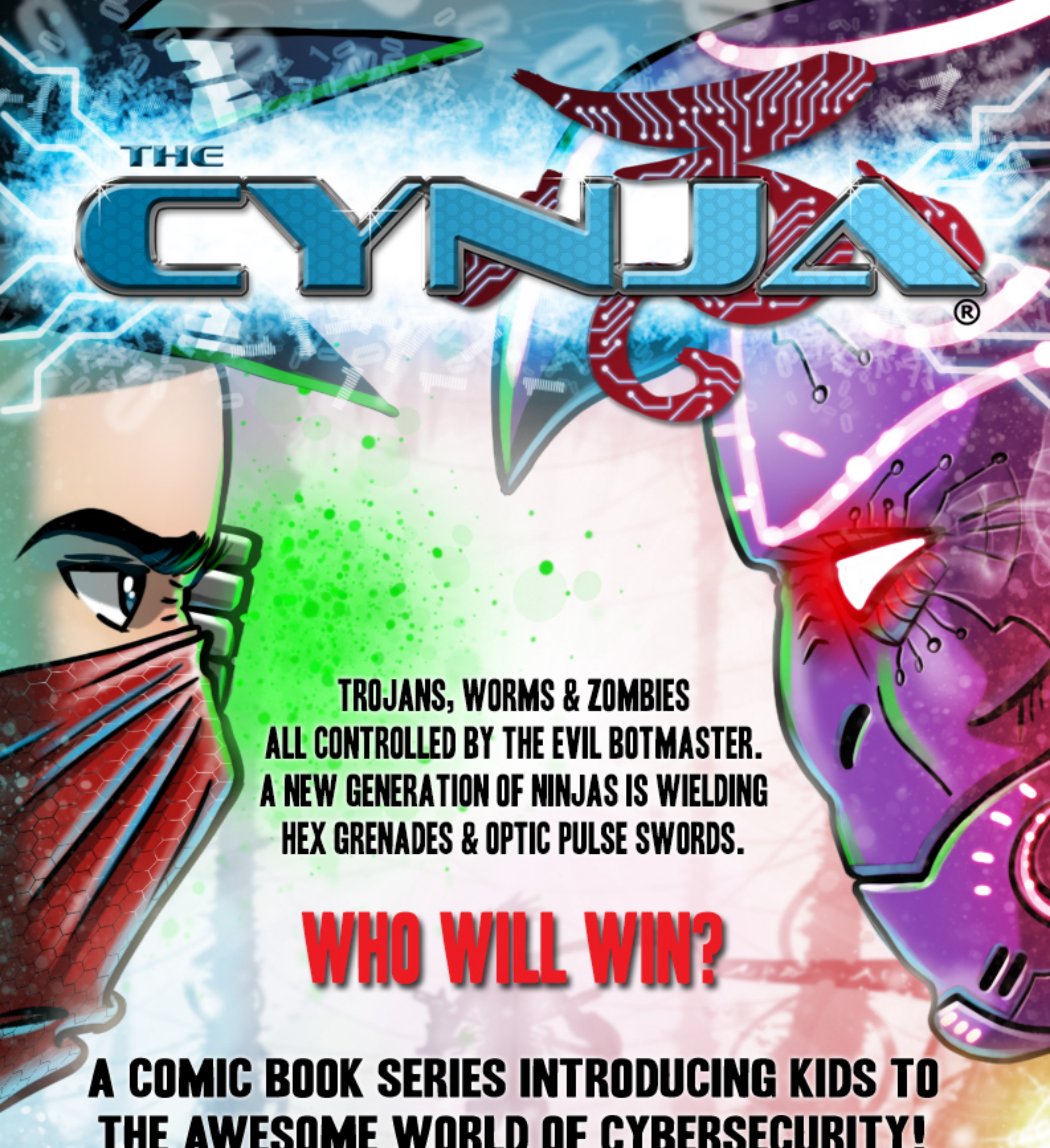
www.mcafeefocus.com/Focus2014/

The Venetian and the Palazzo Congress Center, Las Vegas, USA / 27 October - 29 October 2014

INTERPOL World 2015

www.interpol-world.com

Sands Expo & Convention Centre, Singapore / 14 April - 16 April 2015



THE CYNJA®

TROJANS, WORMS & ZOMBIES
ALL CONTROLLED BY THE EVIL BOTMASTER.
A NEW GENERATION OF NINJAS IS WIELDING
HEX GRENADES & OPTIC PULSE SWORDS.

WHO WILL WIN?

A COMIC BOOK SERIES INTRODUCING KIDS TO THE AWESOME WORLD OF CYBERSECURITY!

WWW.THECYNJA.COM

Big Data analytics to the rescue

by Stephen Dodson

In the battle against cyber criminals, the good guys have suffered some heavy losses. We've all heard the horror stories about major retailers losing tens of millions of credit records or criminal organizations accumulating billions of passwords. As consumers, we can look at a handful of friends at a cocktail party and assume that most, if not all, of them have already been affected.

How can an IT security organization ensure they are not the next target?

It turns out there are common characteristics of successful attacks. However, the evidence of intrusion are often hidden in the noise of IDS/IPS alerts; security teams have no visibility to telltale signs of much of the discovery and capture activities; and exfiltration is cleverly designed to operate below alert thresholds, the traces hidden in huge volumes of data.

These attacks are successful because the security paradigm is based on identifying "known bad" activities and the alert noise generated by that approach necessarily limits the amount of data that can be analyzed.

So how can Big Data analytics help? Think about the amount of operations data generated by a retailer's IT environment. Each device generates operating data at the OS, network, and application layers. There are tens of thousands of PoS devices, network devices, back end servers, middle ware… the list goes on and on. Even a modest sized operation daily generates gigabytes of data, and large enterprises generate well into the terabytes of operations data. Hidden in this data are the fingerprints of intrusion, discovery, capture and exfiltration activities and many of those activities are going to be anomalous.

It turns out that finding anomalies in huge volumes of data is exactly what Big Data analytics approaches, such as unsupervised machine learning, are good at.

Finding the important amid the noise

It would be easy to assume that IT security teams of the enterprises that have been breached were just ineffective or lazy. But that flies in the face of reason. Even a modest size organization can experience tens of thousands of alerts a day from their perimeter defenses. We would have to assume that number to be well into the hundreds of thousands at a large retail organization. Ten thousand of those are likely to be high severity alerts. In fact the vast majority of security architects and CISOs will tell you they simply can't process the alert noise generated by their intrusion tools.

Cyber criminals are well aware of the challenge IT security teams face. They can be fairly confident that alerts generated by their attempts to penetrate a target of worth will go unnoticed in the massive volume of simultaneous notifications.

Some security architects, however, have taken the clever step of running advanced analytics on the alert themselves. It can be a relatively simple exercise to monitor IDS alerts in real-time to uncover an unusual concentration of attacks on a specific target, from a specific source or of a specific type.

The security team at a major digital marketing firm, a prime target for criminals because they house hundreds of thousands of valid email addresses for their clients, did just that. Real-time analysis of hundreds of thousands of alerts generated in a typical week resulted in 5-10 accurate notifications of activities that required special focus.

Finding the suspicious activities inside the perimeter

The “known bad” approach actually limits our security in three ways. First, it requires significant human effort to implement, manage and maintain the threat signatures and rules that trigger alerts because they're constantly evolving. Second, it invariably generates a very high volume of alert “noise.” Third, the amount of manual effort and resultant noise weigh against analyzing other valuable sources of data.

Nowhere is this third impact more noticeable then in the inability of security teams to identify suspicious activities inside their perimeter.

Once an attacker has breached perimeter defenses, they set out to find vulnerable host systems and data stores. Almost invariably, this results in activities that are abnormal. To give a few examples: a new process will appear on a server and connect to the network; systems that usually receive network traffic will start sending; or authorized access users will generate an unusual level of failed passwords or start to access the network from a new device or at an odd time of day.

There are two impediments to successfully finding the “fingerprints” of these activities. The first is the “known bad” approach. Let's take the simple example of scanning internal systems for unusual software processes that are connecting to the network.

This is a particularly useful approach to finding compromised internal systems. The known bad approach would be to identify the specific software processes you are concerned about like FTP. Hackers will expect that you will look for that and so instead they would use the little known PUT capability of HTTP. FTP and HTTP will be normal processes on some servers, so in order not to generate false alarms, your security architect would have to know to which servers these alert rules apply.

When you are talking about hundreds, thousands or tens of thousands of devices, this is simply impractical.

Machine learning algorithms, on the other hand, can easily “learn” the normal activities of hundreds of thousands of servers and tell you immediately when one of them connects to the network with a software process that is unusual for that specific device. It can do so on commodity hardware, with very little setup and none of the required maintenance associated with rules.

Similarly, audit and access logs can be analyzed, again without rules, to immediately identify suspicious access attempts.

Finding the earliest signs of data theft

The fingerprints of data exfiltration are hidden in massive sets of machine data being generated by web proxies and network flow. However, getting usable and actionable information from these data sets has significant challenges.

When the data in question comes from sources such as web proxy servers, the fact that almost all the data within these massive data sets relates to non-malicious, standard business activity is a significant challenge to consider.

Differentiating malicious activity from non-malicious activity is extremely difficult as there may only be a small handful of malicious activities each day that are hidden in the billions of interactions that take place every minute. Generating alerts on non-malicious activity only adds to the cover you are giving to advanced criminal attackers.

Traditional methods of extracting usable information from this data involve searching for known signatures of an attack. Unfortunately, advanced hackers and criminal enterprises know enough to modify the threat signature to avoid detection. In the end, however, the attack is going to generate outlier behaviors, so a complementary approach to signature and rule-based intrusion detection is analyzing internal and outgoing traffic for statistically unusual behavior.

However, the level of statistical analysis required far exceeds the capabilities of even the more advanced security architects or analysts. For instance, there are generally statistically unusual interactions happening all the time in a typical organization. Trying to scan for unusual websites visited by employees of a large enterprise can generate thousands of false alerts per day.

As organizations scale in size, more advanced analyses of interactions across multiple dimensions are required. As an example, the fact that an employee visits a new website only becomes a valid concern if the interaction also involves an unusual protocol for that user and while that user is usually a consumer of data, they are now sending substantial volumes of data in small bursts.

Statistically, modeling data for unusual patterns across multiple dimensions – and doing it accurately – is a complex task even for small data sets, let alone massive data sets. Appropriate modeling techniques and computationally stable and scalable implementations are beyond the scope of simple tools and analyses. Finally, the analysis needs to be executed in real-time, which places additional constraints on the system because it has to be online during the process.

STATISTICALLY, MODELING DATA FOR UNUSUAL PATTERNS ACROSS MULTIPLE DIMENSIONS – AND DOING IT ACCURATELY – IS A COMPLEX TASK EVEN FOR SMALL DATA SETS, LET ALONE MASSIVE DATA SETS.

Staying ahead of the bad guys

Statistical techniques are the only approach that can identify unknown attacks, and even when applied properly will still require a certain amount of human intervention.

Security teams can definitely react a lot faster if they are immediately aware of previously unknown threats, so staying ahead of the bad guys really comes down to two things: the speed of a real-time analysis solution and the reaction time of the security team. In the end, this requires that both the right technology and organizational processes are in place.
As more and more data and data sets become available, the challenge of gaining actionable insight becomes more and more complex. For example, in a smaller office with a couple hundred employees, identifying a user exfiltrating data to an unusual website can be achieved by simple reporting.

However, the same report within a large enterprise that employs thousands or tens-of-thousands of people may contain 500 unusual events per hour, which becomes too large to effectively triage and analyze. As the data increases, effective, accurate and scalable statistical analyses become more and more important as simple reports and rules generate too much information to triage and action.

Since humans are unable to effectively process this volume of information, the only way we'll be able to do it is by relying on machine learning.

While humans become less effective as data sets get bigger, machines actually become more effective, as they have more data to analyze and learn what normal behavior looks like. As a result, they'll become even better at flagging the anomalies. There's no doubt that machine learning will become a much larger part of an effective security strategy as the amount of data increases and becomes even more valuable to an organization.

The importance of security analytics is directly proportional to how much a breach will cost an organization, and in the current environment, they are becoming essential. Amid the perpetual race of hackers looking to break through a perimeter versus security professionals moving to patch the newfound vulnerabilities – and the cycle beginning over again – security analytics have become invaluable.

Stephen Dodson is the CTO at Prelert (www.prelert.com). Prior to software development, Steve worked in the Computational Mechanics group at London's Imperial College, resolving scalability issues using a new approach to solving Maxwell's equations which allowed it to become a practical technique used by major companies.

Why now is the time for enterprises to implement context-based authentication

by Andreas Baumhof

Security and efficiency are constant concerns in enterprise IT. The popularity of BYOD has been a boon for improved productivity and collaboration, but it has also created a new set of challenges, increasing the potential for fraudulent logins from the personal devices that are being used to access critical and non-critical applications.

The level of risk that currently exists in many enterprises is simply not sustainable, since a single security breach can have serious consequences for both brand reputation and the company's bottom line.

To mitigate risk, many enterprises are turning to context-based authentication—a strategy that establishes trust for individual account logins without sacrificing consumer identities or workforce efficiency.

The implementation of context-based authentication can't wait—a combination of increasing BYOD usage and sophisticated BYOD-based attacks have created a sense of urgency around enhanced security strategies. Like it or not, the time to implement context-based authentication is now, before your organization suffers a serious security breach.

The problem with BYOD

When BYOD arrived on the scene, it was enthusiastically embraced by enterprise IT. Instead of spending capital on company-owned devices, forward-thinking IT organizations enabled workers to access specified applications by using personal smartphones and tablet devices. More importantly, BYOD gave employees remote access to critical applications, improving the productivity and efficiency of the workforce.

As BYOD has evolved, employees who use personal devices to access critical applications look and feel like consumers on business websites. This consumerization of IT has created serious security threats, since remote workforce logins are susceptible to many of the same fraud tactics that target consumer-based applications.

The risks associated with BYOD are even more troubling for enterprises that require access for contractors, consultants or partners. Facilitating secure BYOD access for your own workforce is difficult enough, but now many enterprises must provide access to third parties.

To reduce risk, most organizations have implemented traditional access security controls like password verifications—measures that are being phased out because they are archaic and are no longer effective in protecting enterprises from security attacks.

Enterprises must do more to secure applications from unauthorized access, but security isn't the only factor that needs to be considered.

Although the cost of a security breach can be astronomical, managing the cost of enhanced security solutions is also a high priority, especially for IT organizations that are already being asked to do more with significantly fewer dollars.

Likewise, security protocols cannot be so cumbersome that they limit workforce efficiency. In many cases, authentication techniques are so time-consuming that they deter workers from adhering to company policy and motivate them to find workarounds that bypass security altogether.

So, across nearly all industries, enterprise IT faces the difficult task of balancing several conflicting priorities. Enterprises clearly need flexible and robust security technology to prevent account takeovers and other threats. But at the same time, security solutions must be cost-effective and minimize opportunities for the type of friction that reduces workforce efficiency.

Mitigating risk with context-based authentication

Gartner forecasts that by 2016, more than 30 percent of enterprise organizations will leverage context-based authentication to facilitate access for remote workforces.

Why? Because context-based authentication gives enterprises stricter control over employees' devices with a comprehensive process designed to establish trust with devices that access critical enterprise applications.

Unlike traditional security solutions, context-based authentication uses multiple factors to establish trust, preventing account takeovers without impacting user convenience or workforce efficiency. Key factors considered during the user screening process include:

User identities and behaviors: User names, passwords, email addresses, associated devices and other dynamic details about the online behaviors and identities of individuals attempting to access applications.

Device profiles: The identification of anomalies and malware threats linked to the smartphones, tablets, desktops and laptops that are being used for account logins.

Geolocation: Real-time assessment of threat levels based on the country or region from which the login attempt originates.

Custom business rules and policies: Enterprise-specific rules and policies designed to limit BYOD access and create a more secure IT environment.

The use of multiple factors in context-based authentication significantly improves application security because it counters the tactics fraudsters commonly rely on to obtain user credentials, i.e. malware, phishing, shared passwords and other techniques that target simplistic username password solutions.

Tips for implementing context-based authentication technology

BYOD isn't going away anytime soon. In fact, it's likely that BYOD usage will increase as enterprises rely more heavily on third-party contractors and employees push for additional remote work opportunities.

Unfortunately, past IT security investments may not adequately protect the enterprise from BYOD-based threats.

More than ever before, enterprises need to evaluate their current security protocols and solutions, and gauge their ability to securely provide access to users logging in from personal devices.

For many enterprises, the quest for improved application security will culminate with the implementation of context-based authentication technology. With that in mind, there are several features and benefits to look for when selecting a context-based authentication solution:

1. Single sign-ons

User convenience is a critical concern when selecting IT security solutions. Single sign-on systems are designed to give authorized users secure, frictionless access to critical applications from a single login point.

Context-based authentication enables this level of convenience by employing a combination of device analytics, identity analytics, behavior analytics and login context to evaluate whether the login attempt originates from an authentic BYOD user.

2. Access for remote workforces

Enterprises that require application access for third-party contractors need to ensure that their security technology delivers seamless remote workforce access capable of protecting systems and data from unauthorized access.

Additionally, it's important to focus on technologies that allow for the creation of customized business rules and policies for remote workers. In many cases, the customization of business rules serve as the first line of defense against unauthorized access, especially for large and/or diverse workforces.

3. Frictionless two-factor authentication

To maintain the efficiency of your workforce as well as the integrity of your system, login access needs to be both secure and effortless. When users are required to perform multiple steps to log in to applications, productivity suffers and users are incentivized to find ways to bypass security protocols.

The best context-based authentication solutions offer frictionless, multi-factor authentication that passively assesses the trustworthiness of attempted logins—streamlining access for known users that access applications from a trusted combination of accounts and devices.

4. Shared global intelligence

Shared intelligence increases the value of context-based authentication technology by combining multi-factor authentication with a real-time network of data about known, global security threats.

Solutions that leverage a global federated identity network provide the most effective and cost-efficient way to implement security improvements that mitigate enterprise risk and reduce friction for end users.

Although context-based authentication technology won't solve all of your organization's IT security headaches, it's a big step in the right direction for enterprises that rely on BYOD and remote workers for normal business routines.

With new threats emerging everyday, the implementation of a robust context-based authentication solution is more than a logical next step—it's a prerequisite for enterprises that demand agile and reliable access to critical applications.

Andreas Baumhof is the CTO at ThreatMetrix (www.threatmetrix.com). He is is an internationally renowned cybersecurity thought leader and expert with deep experience in the encryption, PKI, malware and phishing markets. Prior to ThreatMetrix, Baumhof was an executive director, CEO and co-founder of Australian-based TrustDefender, a leading provider of security and fraud detection technologies. He previously served as co-founder and chief technology officer of Microdasys, a provider of deepcontent security solutions. While there, he developed the first SSL proxy and has patents pending in Europe and the U.S.

HITBSecConf2014

MALAYSIA

OCTOBER 13th - 16th @ InterContinental
Kuala Lumpur

October 13th & 14th - Technical Training

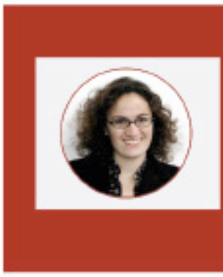
- Understanding x86-64 Assembly for Reverse Engineering & Exploits
- Application Security for Hackers & Developers
- Practical Malicious Document Analysis
- Sensepost Wireless Security Bootcamp
- Practical Threat Intelligence
- iOS Exploitation Techniques
- LTE Security & Insecurity

October 15th & 16th - Triple-Track Conference

Richard Thieme
Founder, ThiemeWorks

Katie Moussouris
Chief Policy Officer, HackerOne

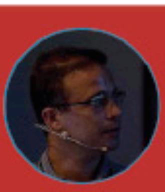
OPENING KEYNOTE
Marcia Hofmann



Marcia Hofmann is an attorney who litigates, counsels, writes, and speaks about a broad range of technology law and policy issues. In 2013 she launched a boutique law practice focusing on computer crime and security, electronic privacy, free expression, and intellectual property. Prior to that, she was a senior staff attorney at the Electronic Frontier Foundation, where she continues to serve as special counsel. She is also an adjunct professor at University of California Hastings College of the Law. She is @marciahofmann on Twitter.

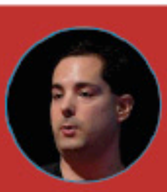
Rosario Valotta

Alban Diquet



Cem Gurkok

Michele Spagnuolo



Don Bailey

Paul S. Ziegler

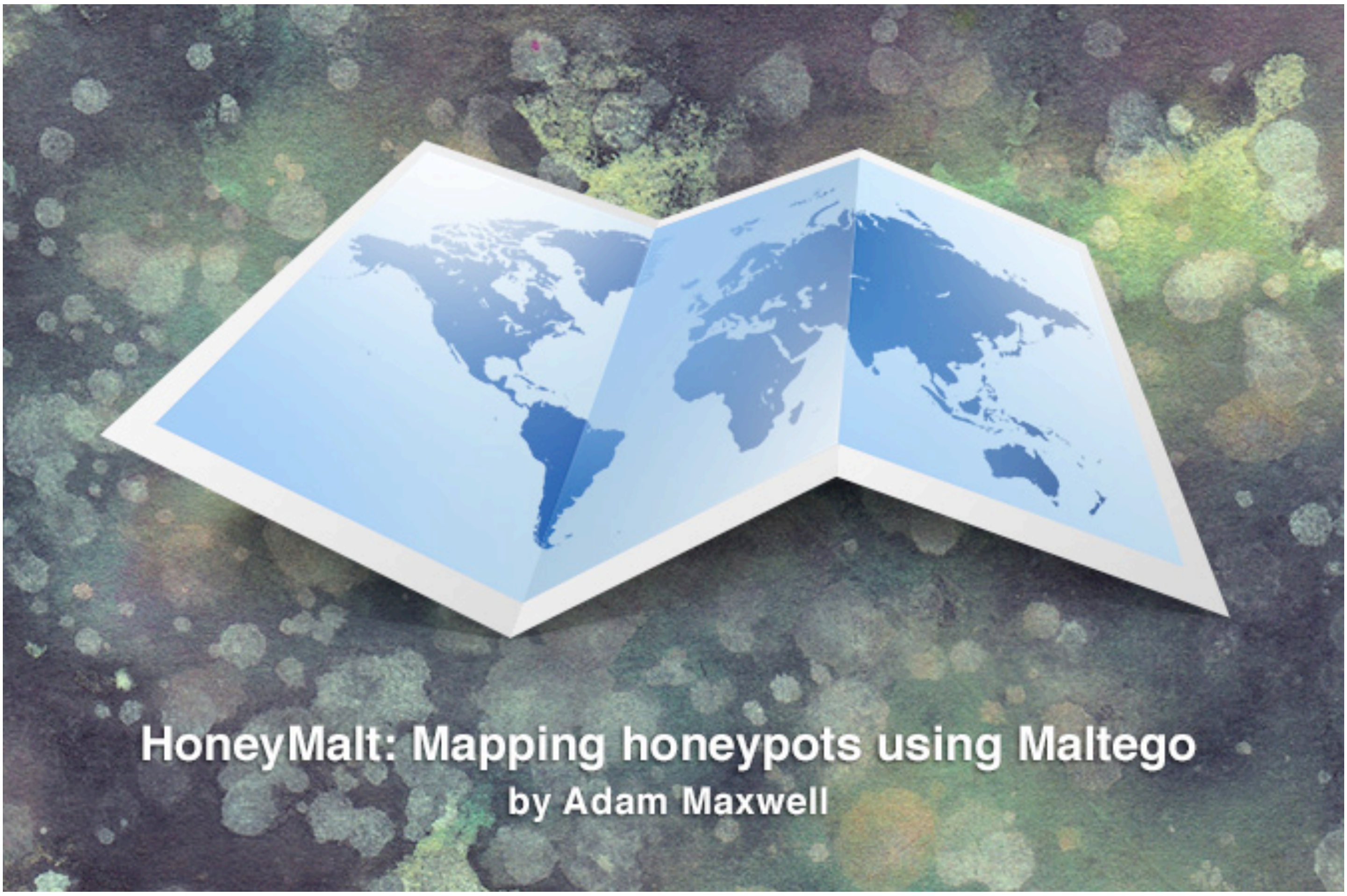
Michael Jordon

REGISTER ONLINE NOW

http://conference.hitb.org/hitbsecconf2014kul/

Follow @HITBSecConf on Twitter for
the latest event updates

The Last HITB Security Conference in Malaysia



HoneyMalt: Mapping honeypots using Maltego

by Adam Maxwell

Not a week goes by without a news story about a security breach in a well-known company, a new malware outbreak, or a group of hackers defacing a high-profile website. Gone are the days when the Internet was primarily a way to share knowledge, learn new things and explore the unknown - now it's a war zone without borders and without rules, with civilian "causalities" littering the ground in the wake of a cyber attack.

Honeypots are one of the tools used by security professionals in this ongoing war. They enable them to gain insight into what the "enemy" is trying to do.

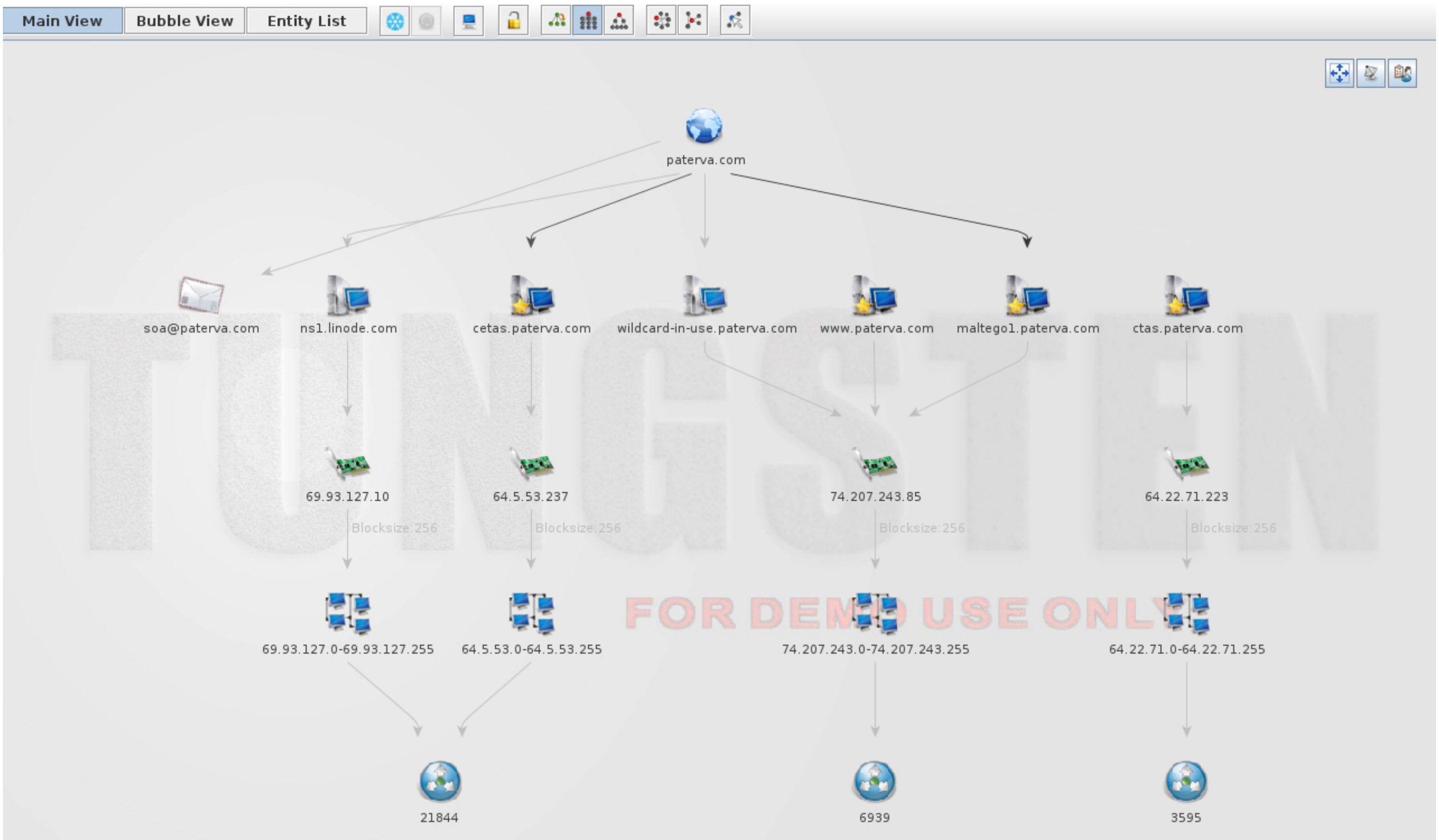
Designed to be vulnerable and made accessible via the Internet, they wait for attackers to connect to them so that they can trap and trick them into giving away their techniques, tools and attack vectors.

Honeypots record everything, providing security professionals with malicious files to analyze, a list of IP addresses to block, and much needed insight into how the enemy operates.

HoneyMalt leverages another tool in the security pros' arsenal called Maltego (www.paterva.com). Labeled as an open source intelligence and forensics application, it visualizes the relationships between numerous sources of data. Maltego makes use of transforms, small snippets of code that execute a function and return an entity (an example of an entity in Maltego is an IPv4 address). These transforms can be extended to provide more functionality and allow users to expand their insight into all kinds of data types.

I have been writing code in Python only for the last year or so. When I started writing Maltego transforms I wanted to do it quickly and not to get bogged down in coding (if you read my code you will understand why).

Luckily, I discovered the Canari Framework (www.canariproject.com), which provides anyone interested in creating Maltego transforms with a quick and easy tool for developing them. By now, I am somewhat addicted to creating custom Maltego transforms.



Whether it's for visualizing honeypots, performing network packet analysis or that of some other random bit of code, the combination of Python, Canari and Maltego (and a sprinkle of imagination) is perfect. Anything you code in Python, you can graph in Maltego.

Now, you're wondering what all this has got to do with HoneyMalt? I run a Kippo SSH (github.com/desaster/kippo) honeypot in the cloud. They are easy to setup and require little continuous maintenance - in fact, it takes more time to look at the logs then it does to keep one running. There are tools that allow you to visualize the information in graphs (bar charts, and so on). You can also query a database directly but, as they say, a picture is worth a thousand words, and that is where HoneyMalt comes in.

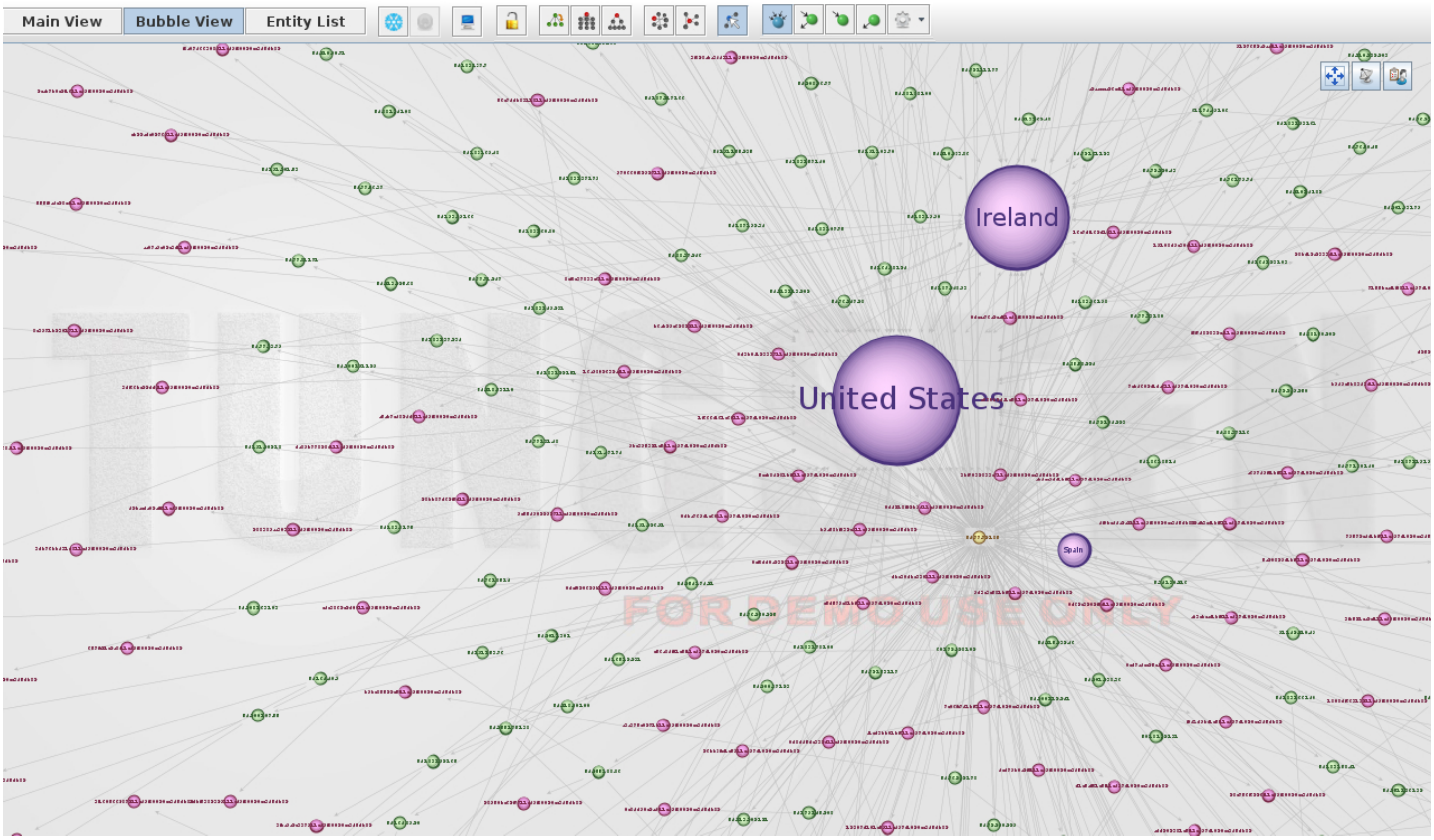
HoneyMalt is a Maltego transform pack built to provide security professionals with the ability to see the data collected in their honeypots in the form of a Maltego graph. It's currently designed to pull information from Kippo-based honeypots, but the number of honeypot types it will work with will soon increase. So far, I have written transforms that return the following entities:

- IP address (Maltego IPv4 entity)
- Geo IP lookup for country code (returns the flag for the country)
- Session ID (HoneyMalt entity, showing unique Kippo session ID)
- Username/password combinations (HoneyMalt entity, showing the username and password the attacker attempted to gain access with)
- Input (HoneyMalt entity, the commands the attacker entered once logged in)
- File download info (Maltego URL entity, shows the URL from which the attacker downloaded some malicious files or tools from).

Let's run through some use case examples:

1. You want to see which country your honeypot gets the most visits from, in relation to the number of connections? Using HoneyMalt and Maltego's bubble view you can easily see which countries are most "active".
2. What's the most common used username/password combination? Maltego's bubble view shows you (see screenshot on the following page).

Data from multiple honeypots and the transforms within HoneyMalt will allow you to see the correlation between multiple sources. For example, if you run honeypots in geographically different locations, and they show the same IP addresses connecting and/or using



the same username/password combination, it's likely that that IP address is a bot, designed to search for vulnerable systems. To make the process of discovering malicious IP addresses and associated sessions easier, I've made use a of Maltego machine. Maltego machines are essentially macros within Maltego that allow for a number of transforms to be executed in a defined sequence. When run, each transform "feeds" the next one with previously returned entities.

The HoneyMalt machine runs every minute to map out your Kippo honeypot for you. The HoneyMalt code is available for download at GitHub (github.com/catalyst256/HoneyMalt), and if you want to see it in action, I've made available a video (youtu.be/1dBptySUMDQ).

Adam Maxwell (www.itgeekchronicles.co.uk) is addicted to Python, pcap and Maltego. He builds infrastructure by day and writes code by night.

Failure is an option

by Brian Honan

Information is the lifeblood of today's business world. With timely and accurate information business decisions can be made quickly and confidently.

Thanks to modern technology, today's business environment is no longer constrained by physical premises or office walls. We can work on laptops, smartphones or tablets and, with nearly ubiquitous internet connectivity, we can work from any location.

With this growing dependence on technology we need to also accept there will be times when that technology is going to fail us, either by accidental or malicious intent. We do not expect 100% security in our everyday lives, and we should not expect it in our "technical" lives. What we need to do is design our systems and security programs to be resilient in the event of a failure. This means shifting our thinking away from solely preventing attacks to trying to develop strategies on how to ensure the business can continue to function should an attack happen and be successful.

In essence, a change in mindset is required, and not just in those developing the security programs, but also in senior business management.

To develop this resilience to cyber-attacks, the focus should be on ensuring the business understands the impact of a potential attack and the steps required for them to prevent, survive and recover from it.

This requires security not to be viewed only as a purely technical discipline, but also from a business and risk management point of view. This requires technical people who would traditionally focus on point solutions to specific technical threats to translate the potential impact of security incidents into terms and language that business and non-technical people will understand.

Business operates on the principle of risk, and every business decision involves an element of risk. Sometimes the result of that risk is positive, for example, increased sales; sometimes it's negative, such as loss of market share. Traditionally, security people with technical backgrounds look at issues in a very black or white way, it either works or it does not work, it is secure or not secure.

Being resilient involves a change in mindset whereby you look to identify how secure the business needs to be in order to survive. This is a challenge for both technical and non-technical people. For business people it requires that they get involved in the decision making process regarding information security security by identifying what are the critical assets to the business and how valuable those assets are.

The risks to those assets then need to be identified and quantified so that measures can be put in place to reduce the levels of risk against those assets to a level that is acceptable to the business. So instead of a checklist approach to security, or an all-or-nothing approach, decisions are more focused on what the business needs and investment can be best directed to the more appropriate areas.

I often compare developing a resilient approach to security to how kings protected their crown jewels in their castles during the Middle Ages. The core of the castle is the keep and it is the most secure part of the castle. The keep was where the most valuable assets were kept. The keep itself was placed in a very defendable position within the castle walls. Those castle walls were defended in turn by moats, turrets, and drawbridges.

Outside the castle walls were where the villagers and farmers lived. In the event of an attack the king would raise the drawbridge leaving those outside open to attack, but these were acceptable losses to protect the crown jewels. Even if the castle walls were breached the crown jewels would remain protected within the keep.

It is time we moved from designing our security infrastructure to avoid failure, and to acknowledge and accept that failure will happen.

In today’s security landscape, businesses need to identify what their crown jewels are and protect them accordingly by moving them to the digital equivalent of a keep. Similarly, they also need to identify what should remain within the village, or even within the castle walls, and be prepared to lose that in the event of a major attack.

Effective security requires rigorous and regular risk assessment exercises, particularly as today the business environments, technology, and security threats, change so quickly. These risk assessments should be supported by good security policies outlining what the required security controls are to manage the identified risks. Key to having a resilient approach to security is to have an effective incident response plan in place so that when an attack happens the business can still function and survive.

It is time we moved from designing our security infrastructure to avoid failure, and to acknowledge and accept that failure will happen. How we deal with that failure will determine how well our organizations can recover from security incidents. Instead of looking how to avoid failure, we need to learn that failure is an option. What is not an option is not being resilient enough to recover from and survive such a failure.

Brian Honan (www.bhconsulting.ie) is an independent security consultant based in Dublin, Ireland, and is the founder and head of IRISSCERT, Ireland's first CERT. He is a Special Advisor to the Europol Cybercrime Centre, an adjunct lecturer on Information Security in University College Dublin, and he sits on the Technical Advisory Board for several information security companies.

Cloud security: Do you know where your data is?

by Steve Pate

The rapid move towards virtualization and cloud infrastructure is delivering vast benefits for many organizations. In fact, Gartner has estimated that by 2016, 80% of server workloads will be virtualized. The reasons are clear: better availability, improved cost-efficiency from hardware investments, and better SLAs.

And while many companies continue their quest to convert their own data centers into true self-service private or hybrid clouds, the growth of public cloud is also undeniable. For companies, the public cloud beckons with unprecedented agility and responsiveness.

For users, the ease of spinning up an environment for a pilot project in a public cloud in a matter of minutes is compelling - especially when compared to month-long wait times many experience when requesting internal server resources from IT.

Yet as research firm Forrester pointed out, “customers initially adopted cloud services to raise business agility at an efficient cost, but increasingly seek to provide new functions for mobile users and modernize their applications portfolios. But concerns about security, integration, performance, and cost models remain.”

Why is cloud security different?

Virtualized infrastructure is the foundation of any cloud—public or private—and virtual workloads need different security. Traditional data centers had natural air gaps, with a set of applications dedicated to each server, a defined administrator for each application, and a defined perimeter around the datacenter. A virtualized datacenter is different.

By nature, a virtual machine is just a set of files, which makes it very easy to copy, suspend and re-instantiate them on any other piece of hardware. This dramatically increases the ease with which someone could either accidentally or maliciously cause application or datacenter downtime, or steal or expose sensitive or confidential data. Further, in a hybrid or public cloud model the definition of “perimeter” changes drastically. Applications and data are no longer physically segmented or contained.

Private and public clouds introduce new concerns around infrastructure security, application and data mobility, and availability and uptime.

What's underneath?

The cool thing about virtualization is that you get better hardware utilization by "floating" applications on a hypervisor. The scary thing about virtualization is that it becomes possible to compromise the hypervisor, which can impact every application running above it. Also, those that manage the virtual infrastructure (or someone who compromises their credentials), have far-reaching privilege, unless the right controls are in place.

Consider the case of Code Spaces, a technology company leveraging Amazon's AWS Infrastructure as a Service cloud to host its applications.

An attacker was able to hack into to the Code Spaces management console in AWS and delete literally every virtual server, putting the company out of business.

For organizations that want to virtualize sensitive or mission critical applications, there are technologies like Intel Trusted Execution Technology (TXT) that can create validation all the way from the chipset through to the hypervisor, ensuring that applications can't boot unless they are on a trusted platform.

The cloud concentrates both applications and data, and therefore if attackers get in, they can reach a treasure trove.

Data sovereignty

The second concern that must be addressed is virtual machine mobility. As you think about the applications you want to virtualize, consider the implications if a virtual machine was copied, or accidentally backed up or replicated to a server outside your data center. Would you risk exposing proprietary company data? Is your organization subject to regulations or mandates that require personally identifiable data be kept inside country or regional boundaries?

Leveraging firewalls, boundary controls, and other technologies, it is possible to re-create the segmentation typically lost with virtualization. For example, a government agency could define policies to ensure that the resources associated with Mission A never cross paths (or administrators) with those of Mission B. Or an organization that is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS) should be able to ensure that applications and PCI data are contained to hardware tagged for this purpose.

Traditionally, organizations have simply not virtualized these types of applications in order to reduce PCI scope. But now it is possible to do so, as long as you have the proper controls in place.

If you're using the public cloud, make sure you understand the service level agreements with your cloud service provider (CSP). CSPs will often replicate virtual machines in the cloud to ensure availability and make sure they maintain their SLAs. Ask them how they are making sure that your apps and data stay where they belong. CSPs should be caretakers, but you ultimately own (and are responsible for) your applications and data.

It's also critical to consider data privacy. The cloud concentrates both applications and data, and therefore if attackers get in, they can reach a treasure trove. Encryption is a proven method to ensure that data remains private, even in the event that someone manages to break through access controls or gain privileged user access.

And make sure your company retains control of the encryption keys, not your cloud service provider. This can also be of value when you wish to change providers or terminate a contract with a CSP.

If the data is encrypted, you can be sure that you're not leaving any sensitive data behind that might be copied from storage devices or other backup systems. Further, encryption can ease the cost, burden and brand damage associated with notification in the unfortunate event you do have a breach, as 48 of the 50 US states have safe harbor clauses in their disclosure laws.

Availability and uptime

Hanlon's Razor states: "Never attribute to malice that which can be adequately explained by stupidity."

The reality is that basic human error accounts for a significant percentage of datacenter downtime. With virtualization, it's far easier for simple errors to have far-reaching impact. For example, a virtual machine can be suspended or deleted with a mouse click.

If that VM is running your credit card processing system, the implications —and cost— can be enormous. IT organizations consistently seek to ensure availability, and for cloud service providers, uptime is mission-critical.

In addition to the basics of hiring good people and maintaining their training, there are some other ways to improve datacenter uptime. Consider implementing controls that can prevent virtual machines from being accidentally or purposely moved to hardware with less performance.

> **Encryption can ease the cost, burden and brand damage associated with notification in the unfortunate event you do have a breach.**

Why it matters

With the cost of breaches growing every year, and the volume of regulations designed to assure the right behavior for companies that handle sensitive data burgeoning, most IT security organizations have reached a fork in the road. They must either choose to make the right investments in technology, people and policy to allow them to continue a secure path to the cloud, or they can choose to maintain the status quo, and risk becoming another headline.

Steve Pate is Chief Architect at HyTrust (www.hytrust.com). He's been designing, building, and delivering file system, operating system, and security technologies for 25 years, and has a proven history of converting market-changing ideas into enterprise-ready products. Before HyTrust, he was CTO and co-founder of HighCloud Security, which was acquired by HyTrust in November of 2013. Prior to that, he built and led teams at ICL, SCO, VERITAS, Vormetric, and others.