(IN)SECURE

Issue 45 - March 2015.

TACKLING TODAY'S AUTHENTICATION COMPLEXITIES

SECURITY AND COMPLIANCE: A BALANCING ACT OF INEQUALITIES

BEST PRACTICES FOR SECURING POS SYSTEMS

TOTAL THREAT PROTECTION: MYTH AND REALITY

HOW DO WE ENSURE THE SECURITY OF THINGS IN LIGHT OF THE INTERNET OF THREATS?

TABLE OF CONTENTS

(IN)SECURE Magazine 45 contributors list

- **Michael Boelen**, founder of CISOfy.
- **Chase Cunningham**, CTO at CynjaTech.
- **Dr. Chris Edwards**, CTO at Intercede.
- **Jason Hart**, Vice President, Cloud Solutions for Identity & Data Protection, Gemalto.
- **Richard Henderson**, Security Strategist at Fortinet's FortiGuard Labs.
- **Numaan Huq**, member of the Trend Micro threat research team.
- **Ken Kartsen**, Senior Vice President of Federal at Intel Security.
- **Slawek Ligier**, Vice President of Product Development at Barracuda.
- **Raj Samani**, Vice President and CTO, EMEA, Intel Security.
- **JD Sherry**, Vice President, Technology & Solutions for Trend Micro.
- **Neha Thethi**, Information Security Analyst at BH Consulting.
- **Wes Withrow**, IT GRC Subject Matter Expert at TraceSecurity.

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

Cisco, Apple, Citrix products no longer welcome on Chinese government systems

A slew of US tech companies have been dropped from China's Ministry of Finance's approved government procurement list, including Apple, McAfee, Citrix Systems and Cisco Systems.

Reuters has had the opportunity to check out the document, and says that Cisco is the biggest loser in this recent restructuring, since an earlier version included 60 of its products, and now none are present.

The Central Government Procurement Center's (CGPC) list hasn't been shortened - in fact, the number of approved products jumped by over 2,000 in the last few years, reaching nearly 5,000. But most of these new additions have been from Chinese manufacturers.

In August last year, Symantec and Kaspersky Lab products have been removed from the list, and the AV software that remained on it was the one developed by Qihoo 360, Venustech, CAJinchen, Beijing Jiangmin and Rising - all China-based companies.

Earlier still, in May, China has announced that it has banned the use of Windows 8 on government computers, but Microsoft still has a foothold on the list - possibly until the Chinese come up with a quality alternative OS based on Linux on which they have been working on.

This latest edit is likely partially due to the revelations stemming from the NSA documents exfiltrated by Edward Snowden. Among other things, they showed that the NSA has apparently been planting backdoors in American-made network devices destined for the foreign market.

Another reason might be retaliation for the fact that Chinese-based manufacturers such as Huawei and ZTE have been branded as suspicious by the US House Intelligence Committee, who urged US companies to avoid using their devices.

But ultimately, part of the reason might also be China's decision to push authorities and companies towards buying local technology, in order to support the domestic tech industry.

Researchers create automated signature compiler for exploit detection

Researchers from Microsoft and University of Erlangen-Nuremberg have created Kizzle, a compiler for generating signatures for detecting exploit kits delivering JavaScript to browsers.

The problem of creating accurate malware and exploit signatures fast is an old one, and this new tool is apparently able to do it within hours of their discovery. What's more, these automatically created signatures are even better that hand-written ones, the researchers found.

"Our approach will reduce the imbalance between the attacker who often only needs to make cosmetic changes to their malware to thwart detection, and the defender, whose role requires much manual effort," they noted in their paper.

By analyzing code found in exploit kits, the researchers noted that while the actual JavaScript delivered by kits varies greatly, the code - after being sufficiently unpacked and de-obfuscated - shows much less variety. The fact that exploit kit authors often reuse much of the code from old kit versions in newer versions allows Kizzle to quickly respond to superficial but frequent changes.

"At the heart of Kizzle is a malware clustering approach that matches new malware clusters with previously-recognized malicious clusters by understanding the process of malware unpacking," they explained. These clusters are the basis on which Kizzle creates AV signatures.

The tool is designed to run in the cloud, and is capable of analyzing large volumes of streaming data. Also, to be clear, Kizzle focuses on making signatures for exploit kits only. However promising their results seem to be, the researchers added that their work and additional testing has just begun, that their current results are limited, and that there are a number of issues to be solved and parameter values to be adjusted.

Known weaknesses plague the security threat landscape

Well-known issues and misconfigurations contributed to the most formidable threats in 2014, according to HP Security Research.

“Many of the biggest security risks are issues we’ve known about for decades, leaving organizations unnecessarily exposed,” said Art Gilliland, senior vice president and general manager, Enterprise Security Products, HP.

44 percent of known breaches came from vulnerabilities that are 2-4 years old. Attackers continue to leverage well-known techniques to successfully compromise systems and networks. Every one of the top ten vulnerabilities exploited in 2014 took advantage of code written years or even decades ago.

Server misconfigurations were the number one vulnerability. Over and above vulnerabilities such as privacy and cookie security issues, server misconfigurations dominated the list of security concerns in 2014, providing adversaries unnecessary access to files that leave an organization susceptible to an attack.

Additional avenues of attack were introduced via connected devices. In addition to security issues presented via Internet of Things (IoT) devices, 2014 also saw an increase in the level of mobile malware detected. As the computing ecosystem continues to expand, unless enterprises take security into consideration, attackers will continue to find more points of entry.

The primary causes of commonly exploited software vulnerabilities are defects, bugs, and logic flaws. Most vulnerabilities stem from a relatively small number of common software programming errors. Old and new vulnerabilities in software are swiftly exploited by attackers.

Superfish not the only app using Komodia's SSL-busting code

As Lenovo backtracked on its initial position that the Superfish adware pre-installed on some of its notebooks is not a security danger, and released a security advisory about the "vulnerability" that allows it to install a self-signed root certificate in the local trusted CA store, Superfish CEO Adi Pinhas did the same.

After first saying that the Superfish software does not present a security risk because it does not "store personal data or share such data with anyone," Lenovo CTO Peter Hortensius shifted the blame to Israel-based Komodia, whose SSL decryption library was used by the Superfish add-on. Pinhas said that the "vulnerability was introduced unintentionally by a 3rd party."

US-CERT has issued a security alert warning about the adware, and pointed out that "the underlying SSL decryption library from Komodia has been found to be present in other applications, including KeepMyFamilySecure."

"In multiple applications implementing Komodia's libraries, such as Superfish Visual Discovery and KeepMyFamilySecure, the root CA certificates have been found to use trivially obtainable, publicly disclosed, hard-coded private keys. Note that these keys appear to be distinct per application, though the same methods have proven successful in revealing the private keys in each instance," they explained in a vulnerability note about the Komodia Redirector with SSL Digestor.

"In addition to sharing root CA certificates across installation, it has been reported that the SSL validation that Komodia itself performs is broken. This vulnerability can allow an attacker to universally attack all installations of Komodia Redirector, rather than needing to focus on a single application / certificate."

Matt Richard, a Threats Researcher on the Facebook Security Team, also shared the results of a project they started with researchers from Carnegie Mellon University to measure how prevalent SSL MITM was in the wild, and has pointed out that there are a dozen other software applications using the Komodia library, and that many of them appear to be suspicious.

"We can’t say for certain what the intentions of these applications are, but none appear to explain why they intercept SSL traffic or what they do with data," he noted, adding that there is also malware out there using Komodia's libraries to break SSL encryption.

Antivirus provider Lavasoft has also shared that its Ad-Aware Web Companion software also used to rely on Komodia’s SSL Digestor for inspecting HTTPS traffic, but that it has been removed in the newest version.

Researcher Johannes Böck found the Privdog adware, shipped with software from Comodo, to be worse than Superfish:

"A quick analysis shows that it doesn't have the same flaw as Superfish, but it has another one which arguably is even bigger. While Superfish used the same certificate and key on all hosts PrivDog recreates a key/cert on every installation. However here comes the big flaw: PrivDog will intercept every certificate and replace it with one signed by its root key. And that means also certificates that weren't valid in the first place. It will turn your Browser into one that just accepts every HTTPS certificate out there, whether it's been signed by a certificate authority or not. We're still trying to figure out the details, but it looks pretty bad."

THE UNDERLYING SSL DECRYPTION LIBRARY FROM KOMODIA HAS BEEN FOUND TO BE PRESENT IN OTHER APPLICATIONS

How cybercriminals hack our brains

Cybercriminals are increasingly using persuasion techniques in order to manipulate employees to do things they normally wouldn't, usually resulting in the loss of money or valuable data.

Intel Security reveals some of the basic persuasion techniques currently in use by cybercriminals, which all businesses and employees should be aware of:

1. Reciprocation: When people are provided with something, they tend to feel obligated and subsequently repay the favor.

2. Scarcity: People tend to comply when they believe something is in short supply e.g. a spoof email claiming to be from your bank asking the user to comply with a request or else have their account disabled within 24 hours.

3. Consistency: Once targets have promised to do something, they usually stick to their promises because people do not wish to appear untrustworthy or unreliable. For example, a hacker posing as a company's IT team could have an employee agree to abide by all security processes, and then ask him / her to perform a suspicious task supposedly in line with security requirements.

4. Liking: Targets are more likely to comply when the social engineer is someone they like. A hacker could use charm via the phone or online to 'win over' an unsuspecting victim.

5. Authority: People tend to comply when a request comes from a figure of authority. This could be a targeted email to the finance team that might appear to come from the CEO or President.

6. Social Validation: People tend to comply when others are doing the same thing. For example, a phishing email might look as if it's sent to a group of employees, which makes an employee believe that it must be okay if other colleagues also received the request.

Windows 10 will offer password-free authentication

The upcoming Windows 10 will offer more authentication options instead of just passwords, Dustin Ingalls, Group Program Manager for Windows Security & Identity, has shared in a blog post.

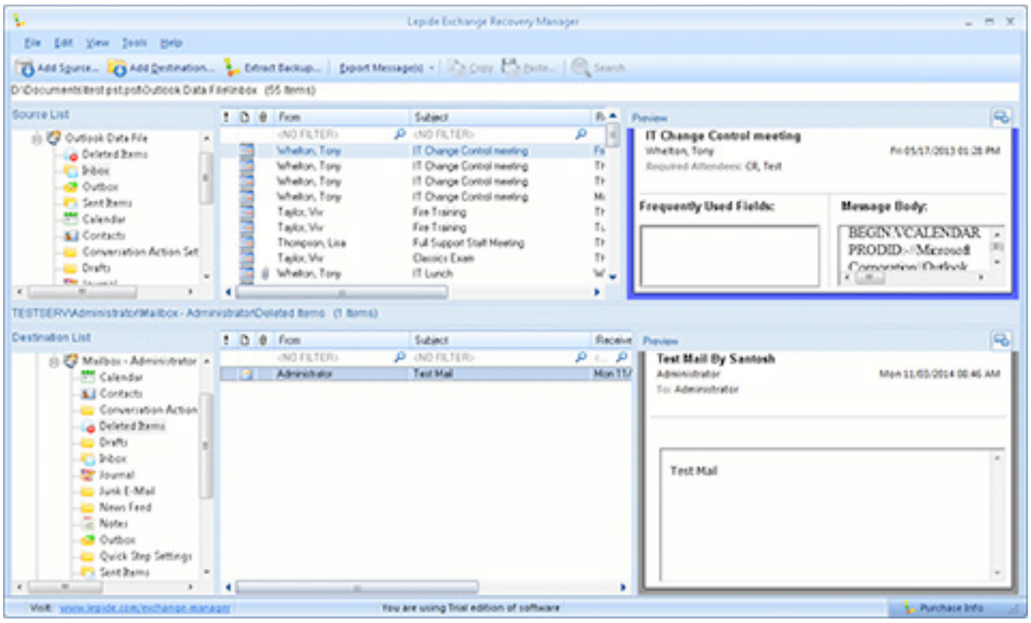
"I'm happy to announce Microsoft has contributed design inputs to the FIDO Alliance, to be incorporated within FIDO 2.0 Technical Specifications. Transitioning away from passwords and to a stronger form of identity is one of the great challenges that we face in online computing, and we believe FIDO authentication [...] is the pathway to success," he said.

"Our current implementation in the Windows 10 Technical Preview reflects our inputs into the FIDO 2.0 Specification Technical Working Group and members of the Windows Insider Program can start evaluating it right away," says Ingalls.

"The current Technical Preview build enables a number of enterprise scenarios and it showcases our integration with Windows 10 sign-in, Azure Active Directory, and access to major SaaS services like Office 365 Exchange Online, Salesforce, Citrix, Box, Concur, just to name a few. With Windows 10, for the very first time Windows devices and Microsoft-owned and partner SaaS services supported by Azure Active Directory authentication can be accessed end-to-end using an enterprise-grade two-factor authentication solution – all without a password."

It's still unknown what specific authentication options Windows 10 users will have.

So far, the Universal Authentication Framework involves biometrics, and Universal Second Factor uses a physical USB device. Google has already implemented the latter in order to offer an alternative second factor for its two-step account verification option. But, according to FIDO's plans, NFC and Bluetooth extensions are likely to be completed in 2015.



D:\Documents\test pst.pst\Outlook Data File\Inbox (55 items)

From	Subject	R
<NO FILTER>	<NO FILTER>	
Whelton, Tony	IT Change Control meeting	Fr
Whelton, Tony	IT Change Control meeting	Th
Whelton, Tony	IT Change Control meeting	Th
Whelton, Tony	IT Change Control meeting	Mo
Taylor, Viv	Fire Training	Th
Taylor, Viv	Fire Training	Tu
Thompson, Lisa	Full Support Staff Meeting	Th
Taylor, Viv	Classics Exam	Th
Whelton, Tony	IT Lunch	W

IT Change Control meeting
Whelton, Tony Fri 05/17/2013 01:28 PM
Required Attendees: CR, Test

Frequently Used Fields:

Message Body:
BEGIN:VCALENDAR
PRODID:-//Microsoft
Corporation//Outlook

TESTSERV\Administrator\Mailbox - Administrator\Deleted Items (1 items)

From	Subject	Receive
<NO FILTER>	<NO FILTER>	<...
Administrator	Test Mail	Mon 11/

Test Mail By Santosh
Administrator Mon 11/03/2014 00:46 AM
To: Administrator

Test Mail

Visit: www.lepide.com/exchange-manager You are using Trial edition of software

Lepide Exchange Recovery Manager 15.0 released

The latest version of Lepide Exchange Recovery Manager (www.lepide.com) allows users to add Office 365 as Source directly in Lepide Exchange Recovery Manager. Once added, the users can perform the usual operations as they used to perform on other sources such as:

- Migrate an Office 365 mailbox or its content to PST, any Live Exchange Server, or the other Office 365
- Use inbuilt nested search to find the exact required emails
- Generate reports for important aspects to keep a check on the contents
- Export emails from Office 365 to EML or MSG files
- Copy the contents of Office 365 and paste it in any destination.

A user can migrate multiple or all mailboxes at once from any Exchange Server or Office 365 to PST files. By default, one PST file is created for one mailbox except for the cases where size restriction of a PST file is applied.

GPG development will continue as donations pour in

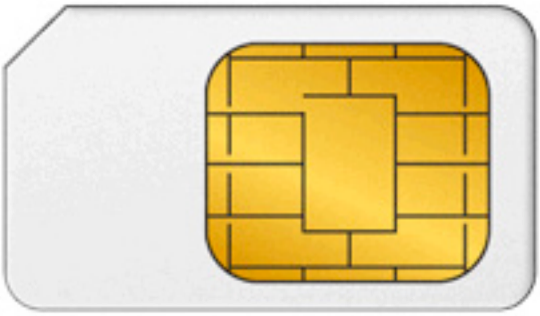
An article by Julia Angwin on ProPublica has become the catalyst for an avalanche of much needed donations for the survival of Gnu Privacy Guard.

GnuPG is a free implementation of the OpenPGP standard, and allows users to encrypt and sign their data and communication. It's a command line tool that can be easily integrated with other applications. The software was built in 1997 by Werner Koch, who through the years and with the help of employees and volunteers kept the software updated and working. But the project was sustained by donations, and through the years they dried up.

Koch resolved to stop working on the software in early 2013, but after Edward Snowden's revelations, he decided to continue because "this was not the time to cancel." Snowden himself was a GPG user, and made a guide for journalists on how to use it. Koch started a donation drive early last year, but until the end of November he received less than 7,000 € (his goal was 120,000).

"Due to this ProPublica article we received more than €120,000 of individual donations on a single day. The Core Infrastructure Initiative granted 60,000 $ for 2015. Our payment service Stripe and Facebook will each give $50,000 to the project. And finally the Wau Holland Stiftung is collecting tax deductible funds for GnuPG (€ 7000 in December; numbers for January will be posted soon)," he shared on the project's website.

The great Gemalto SIM heist



A set of documents from Edward Snowden's trove indicate that the US NSA and the UK GHCQ have managed to compromise the networks of Dutch SIM card manufacturer Gemalto and acquire encryption keys that protect the privacy of cellphone communications of millions of users around the globe.

Intelligence agencies in possession of these keys would be able to eavesdrop on voice calls, text messages and Internet activities of users who's mobile phones work with one of these SIM cards, without the need to break the crypto that protects them and without requiring mobile network operators to give them the required access to do so.

Gemalto is one of the biggest chip makers in the world, and provides them to over 450 wireless network providers around the world, including the US.

The attack, mounted together by the two security agencies, was allegedly successfully executed in 2010, and the attackers managed to hide any evidence of them having been inside the company's network. Most of the keys were stolen by compromising email accounts of employees of Gemalto and mobile network operators, as the encryption keys for the SIMs are often sent via email or through FTP.

According to the leaked document, the GCHQ was also preparing to target German SIM card manufacturer Giesecke and Devrient with a similar attack.

Less than a week later, Gemalto has released the results of an internal investigation into the issue.

"The investigation into the intrusion methods described in the document and the sophisticated attacks that Gemalto detected in 2010 and 2011 give us reasonable grounds to believe that an operation by NSA and GCHQ probably happened," they stated.

The company noted that they, as a digital security company, experience a lot of attacks and that looking back at the period covered by Snowden's documents, there were two "particularly sophisticated intrusions" that could have been effected by the intelligence agencies.

But they say that these intrusions affected only their office networks, and that SIM encryption keys and other customer data are not stored on those networks. "No breaches were found in the infrastructure running our SIM activity or in other parts of the secure network which manage our other products such as banking cards, ID cards or electronic passports. Each of these networks is isolated from one another and they are not connected to external networks," they reassured.

All of this makes them believe that the agencies "chose to target the data as it was transmitted between suppliers and mobile operators as explained in the documents."

Since well before 2010, Gemalto uses "highly secure exchange processes" when sending and receiving SIM data, they added, but at the same time "these data transmission methods were not universally used and certain operators and suppliers had opted not to use them."

They also pointed out some discrepancies in the report that indicate that the NSA and GCHQ targeted other parties besides them: targeted operators with whom they didn't do business with, locations of personalization centers that they didn't operate at the time, etc.

Finally, they tried to reassure that 3G and 4G cards could not have been affected by the attack.

But the speed with which they came out with these results has had security experts question the accuracy of the findings.

How do we ensure the Security of Things in light of the Internet of Threats?

by Richard Henderson

IDC estimates that by 2020 there will be well over 200 billion "things" connected to the Internet in some fashion. We know that connected devices are creating an Internet of Threats. So how do we ensure the Security of Things?

In many cases, these devices were not designed with security in mind and some were never meant to be connected to a network. Bolt-on solutions by vendors have created remarkable levels of productivity and efficiency gains. During an oil exploration operation in a remote area, for instance, engineers can now query devices from literally thousands of miles away before determining if a visit to the location is required. But with these amazing gains comes significant risk: devices with hardcoded authentication credentials or fully documented backdoors are a reality.

What can we do to ensure that security plays a key role in today and tomorrow's explosion of device connectivity?

Protecting devices in the enterprise and in industry

On the enterprise side, as well as in environments like heavy industry and public utilities, there are some key points to remember when designing and deploying solutions.
Many devices are designed with lifecycles measured in years, if not longer, and those devices may be built with machine-to-machine (M2M) communication in mind, meaning some devices may never have a set of human eyes monitoring them for anomalous behavior.

To protect these devices, it's important to deploy a solution that involves some or all of the following:

Hardware-based firewalls/gateways: By deploying a hardware security device between the Internet and your IoT devices, you add an additional layer of security that can prevent an attacker from gaining access to your devices. Hardware-based security tools designed with IoT in mind are much more agile and quick to respond to new and emerging threats.

Strict whitelisting: In many IoT environments it's not likely that your device is going to need to have access to more than a few different resources. If your devices allow it, a very strict whitelist may prevent unauthorized access or tampering.

Secure boot: Devices can use digital signatures to verify the integrity of device firmware when a unit boots or reboots. Choosing solutions that implement this feature can ensure that software or firmware that's been properly signed by the vendor is the only code that can run on the device.

Proper architecture design: Gone are the days of flat networks that you just throw everything onto and plug into your switching and routing infrastructure. By keeping your IoT devices segmented from other parts of your intranet, you reduce the risk of attacks that pivot from your IoT devices into your regular network, or vice-versa.

Choose solutions that vendors commit to patching: I believe we will soon reach a watershed moment when it comes to IoT security. Initiatives like I Am the Cavalry and BuildItSecure.ly are convincing device manufacturers to get on-board with secure development, proper vulnerability disclosure processes, and commitments to patching critical vulnerabilities.

Apply regular network security principles to IoT: Decision makers and solution implementers/designers need to remember that even though there are unique pieces to IoT, many of the basic network security rules and best practices still apply. When you consider compliance-based rules like PCI-DSS and HIPAA, securing your devices that transmit payment data or confidential patient records require extra attention. Do your devices properly secure the data in transit when they send it to other systems? Are they using robust, difficult to break encryption standards? Encryption has a very real cost when it comes to IoT. While processing overhead and available resources have exploded so much in normal computing that high-overhead encryption technologies are no longer "nice to have," IoT devices tend to have low power processors and relatively small amounts of memory, which makes deploying heavy encryption difficult to justify. If you're dealing with the kind of data that requires an extra level of protection, make sure to factor that cost into your purchasing equations.

Regular auditing: Any security professional worth his or her salt will tell you that regular penetration testing is one of the most effective tools in their toolbox. Extending your regular security audits to include your IoT devices is critical. If that kind of testing is beyond your day-to-day skills, bring in an outside professional or take the time to build those skills. Remember: IoT devices usually don't take well to being hammered on, aggressive fuzzing or denial-of-service testing. Make sure you fully define the scope of your IoT tests before you accidentally take something down that might be critical to your business. And don't forget physical security!

It's a bit different on the consumer side. What can a home user do to protect their home networks from IoT-based threats? There are a few key pieces:

Segment your network: Keep your IoT devices on a segmented network. The prices of home routers are so small now that it shouldn't be difficult to physically separate your devices from your computers, which likely contain important files like family pictures and financial documents. If you can't deploy a second NAT router inside your network, consider a router that allows installation of third party router firmware. For example, DD-WRT provides significant functionality above what your router was originally designed for.

Choose devices that are designed with patching and security in mind: Remember, many device manufacturers are well on their way to designing the next generation of devices once the latest model hits the shelves. Many of these companies have little interest in going back to a device a couple of years old in order to patch in a recently-found vulnerability. Choose vendors who have put the responsibility of security beyond their next quarterly earnings report.

IoT is here to stay. It is up to you to fully consider all the pieces of the puzzle when deploying solutions. A multi-layered and robust security architecture will go a long way to ensuring your critical systems don't get taken down or are used as a launching pad into the rest of your network.

Richard Henderson is the Security Strategist at Fortinet's FortiGuard Labs (www.fortiguard.com).

Security and compliance: A balancing act of inequalities

by Wes Withrow

At some point in every IT security professional's career, they will be asked for their opinion on the merits of compliance and how soon it will be before compliance frameworks get to the point that organizations are "hack proof."

The response almost invariably goes like this: "Compliance isn't perfect but at least it's forcing us to talk about security. Nothing is hack proof unless it's powered off, unplugged from the network, and destroyed with hammers. Even then your data probably got synced to your fridge without you knowing."

This provides us the window of opportunity to explain the difference between being compliant and being secure. Compliance and security weren't designed to be packaged and sold as the same product. Somewhere in the chaos of the last decade it was falsely engrained in people's minds that companies who protected their data with compliance-driven security programs were immune to cyber breaches.

Moving beyond compliance-driven security strategies

Compliance-driven security is a strategy that is less concerned about improving the security posture of an organization and more about quickly "checking the box" to keep regulators at bay. It's the "D minus" equivalent of passing the bar exam and telling yourself that you're a great attorney now that you've passed.

The alternative solution that is gathering momentum is a risk-based approach to security. This is the practice of embedding IT security within the organization as a process and not as a checklist. Organizations who practice risk-based security continuously identify, evaluate, prioritize, and balance risks as they change over time. Compliance never goes away with this approach, it just gets folded into the process.

Compliance has historically been viewed as a painful activity that companies responded to with a "one day of the year" mindset that usually involves a lot of scrambling to figure out the most basic information about their networks. In contrast, risk-based security has been looked at as the ongoing process that addresses the rest of the 364 days of the year. Being compliant becomes a byproduct that, over time, eliminates the scrambling.

Heightened visibility changes the security perception

Why does it feel sometimes as if the state of IT security has gotten worse since compliance came around? It's not that it's actually worse; it's more of a case where the gaps in IT security are being exposed in alarming ways and now have everyone's attention.

To understand it more clearly, let's first get some historical context on why compliance frameworks exist, and then discuss a major contributing factor that continues to widen the gap between our compliance and our security.

Legal and regulatory compliance frameworks usually originate from necessity. That necessity usually surfaces as the result of an extraordinary event or trend whose catastrophic failure is rooted in a "not my problem" mentality that won't fix itself. (Whether we agree on the effects of regulation or not is not the purpose of this discussion; let's agree that this discussion is about the necessity of security and not how to perfect it.)

IT security mandates were never meant to act as a blunt instrument of oppression; they were designed to act as a subtle nudge to point out the obvious: the cost of inaction will always outweigh the cost of action.

For years compliance-driven security initiatives have been shuffled to the bottom of the deck of priorities while companies weathered the economic recession. When organizations were told that they had to take "reasonable and appropriate measures" to secure their data, "reasonable and appropriate" was interpreted as a battle-cry that was conveniently favorable to not doing much at all. Herein lies the primary problem, and why being compliant and being secure is not the same thing.

LEGAL AND REGULATORY COMPLIANCE FRAMEWORKS ORIGINATE FROM NECESSITY

Offensive capabilities are a business inhibitor

Shifting gears away from the historical view to a more strategic view, the widening gap that exists between "being compliant" and "being secure" exists because most nations have been focused on developing their offensive capabilities (e.g. infiltration, espionage). It has been an all-hands-on-deck focus on supporting a digital arms race where attacks are developed, deployed, and many times knowing that there's almost always collateral damage as a result.

The odd phenomenon about a compliance-driven or reactive strategy is that the trickle-down effect that provides some military or economic advantage is often times wiped out by the collateral damage inflicted on everyone. That's the nature of pure offense in this game.

It's somewhat analogous to high scoring football games. In football, a hurry-up offense is a fast-paced strategy where the team with the ball runs plays in rapid succession with the goal of outscoring their opponents through pure offensive dominance. Fans whose teams run hurry-up offenses love the games they win and are miserable during the games they lose.

When your offense scores 65 points a game and your defense gives up 66 points a game, you always lose. The loss almost always seems inevitably scripted with a rough ending.

The approach to cyber is similar in the sense that the world's most powerful nations have been running hurry-up offenses against each other for years with little focus on defense. This run-and-gun digital arms race has resulted in an unbalanced scenario where the game clock never stops and the defense never has time to catch their wind.

The focus on offense advances so quickly that collateral damage inflicted on your own team is an expected outcome of a good game.

Cyber attacks have had some benefits though, albeit very few up until more recently when compliance penalties caused financial impact.

Without the financial penalties associated with breaches, there's little to no incentive for spending on security and an even lower threshold for reporting on what happens when companies get breached. Our response when compliance is inadequate? Apply more compliance, of course.

Hyper-compliance bridges the gap

Hyper-compliance is a relatively new term applied to an era that we've just begun to embark upon. This era is characterized by the fast-paced acceleration of pressure by both regulators and customers on businesses to secure data to the point where people become so overwhelmed with how to respond that they lose focus on why they are responding. It's part frustration and part confusion.

For example, what regulations apply to our company now? What regulation trumps the other? What is more important, PCI-DSS or GLBA? The list of questions goes on and on in an infinite loop.

WITHOUT THE FINANCIAL PENALTIES ASSOCIATED WITH BREACHES, THERE'S LITTLE TO NO INCENTIVE FOR SPENDING ON SECURITY

The era we're facing is less about major rewrites of compliance frameworks and more about rapid enforcement and change to how companies approach IT security. Regulations that were once avoidable and unenforceable will now be mandatory and applied more liberally than in the past.

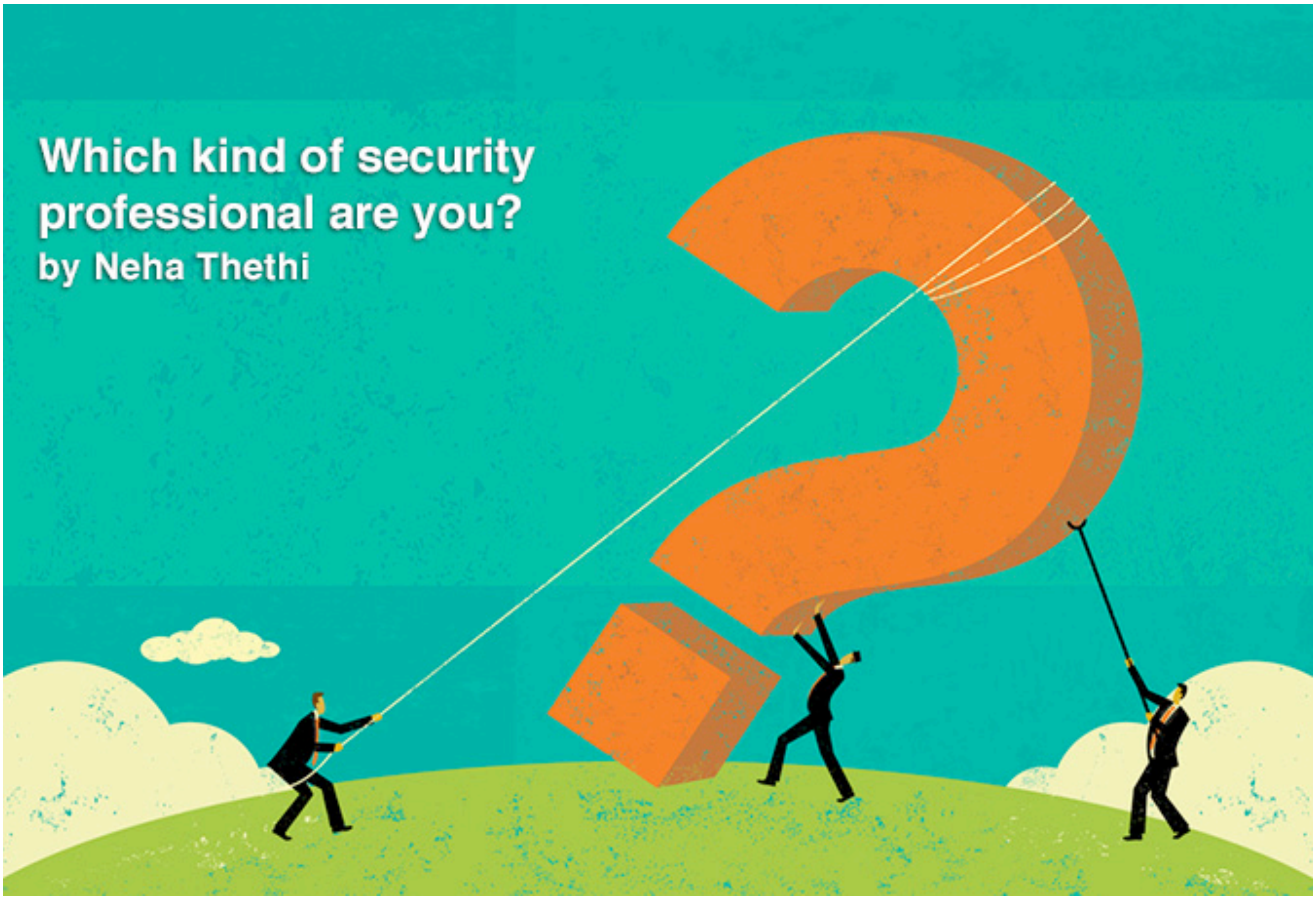
The business-to-business risk evaluation process that companies didn't have to address in the past will be implemented in contract vehicles and new service agreements in the future. Again, view this as positive but painful change.

The list of changes over the horizon goes on and on, most for the better and some for the worse. Albeit painful at times, this type of vigilant compliance with an increased focus on security will help bridge the gap between people's understanding of what being compliant versus what being secure means.

Wes Withrow is the IT GRC Subject Matter Expert at TraceSecurity (www.tracesecurity.com), a provider of cloud-based security solutions that deliver end-to-end IT governance, risk and compliance management capabilities for organizations of any size, industry or security expertise.

Which kind of security professional are you?

by Neha Thethi



Much has been said and written about the arrogance prevalent in the computer industry, especially that of gamers and security professionals.

A well-known female gamer recently felt compelled to launch an anti-harassment support network after being harassed online, being subjected to doxing and bullying, and receiving death threats over the Internet. Other women have withdrawn from the gaming industry altogether.

(Some) security professionals are arrogant, too. For those unaware of this, just google “computer security arrogance."

Since I became a part of the industry, I had to decide what kind of a security professional I wanted to be – humble or arrogant. When new to a community or a group, you look up to the leaders - the supremos - for inspiration. Fortunately, I came across recognized and very humble security professionals, and I then knew what I stood for.

Whether or not I have achieved the desired level of humility is a different story, but what's important is that I'm willing to work on it.

Arrogance is defined as "having or displaying a sense of overbearing self-worth or self-importance. Marked by or arising from a feeling or assumption of one's superiority toward others." Arrogant individuals are also called haughty, disdainful, supercilious.

What does your inner voice say? Which kind of a professional are you? Are you arrogant, haughty and superior? Or humble, modest and respectful?

To help you decide, here are a few indicators. You are arrogant if you avoid eye contact, interrupt conversations frequently, have an answer for everything, drop names out of context, arrive consistently late to meetings and don't apologize, use condescending phrases and put-downs, have a dominating body language when you walk into a room, always ahead of the other person, bad-mouth competitors and blame someone else for your mistakes.

SOME BELIEVE THAT HUMILITY IS A SIGN OF WEAKNESS AND ARROGANCE A SIGN OF STRENGTH.

Some believe that humility is a sign of weakness and arrogance a sign of strength. However, the world has seen leaders of all kinds. Let’s delve a bit into history, politics and philosophy.

The humble one

George Washington was a humble leader. He considered his role of president of the United States as that of a public servant rather than a mighty ruler. A living example of humility is José "Pepe" Mujica - the president of Uruguay since 2010. He has, in fact, been described as "the world's 'humblest' president", due to his austere lifestyle and his donation of around 90 percent of his monthly salary to charities. He also believes a president is a civil servant and not a king.

The arrogant one

One of the most acclaimed leaders in the history of the world was Alexander the Great, a young Macedonian king who believed that ability, focus, and determination would enable him to conquer the world. By age twenty he became king and by twenty-six master of the entire eastern half of the ancient world. But, each successive conquest along with the power and wealth that came with it bred arrogance in him instead of caution, moderation, and reflection.

THINK ABOUT WHAT YOU WANT TO BE KNOWN FOR AND INSPIRE OTHERS BY YOUR ACTIONS.

The one who acknowledged the problem

Benjamin Franklin - writer, politician, scientist, and the connector of people and ideas, went on a quest for "moral perfection" and found that humility, however elusive, proved worth the effort even though he didn't succeed at perfecting it. To make himself seem more humble, he used phrases such as "I conceive" or "I apprehend" rather than "certainly," "undoubtedly," etc.

Some critics argue that he was mocking the 18th-century optimism, which promoted the belief in the perfectibility of man, while others seemed convinced his efforts were genuine. Either way, Franklin seemed to be clearly aware of the humility vs. arrogance problem.

Even if you’re not a leader or a CIO or a CISO, you need to acknowledge the problem and strive to achieve humility. Think about what you want to be known for and inspire others by your actions. Great leaders or professionals don't need to act tough as their confidence and humility serve to accentuate their toughness.

It is very important to remember there is a difference between confidence and arrogance. I believe this quote sums it up well:

"Some say there is a fine line between confidence and arrogance; I think just the opposite. Confident people are secure with themselves while arrogant people are insecure and have to boast to get acceptance from others." - Kamari aka Lyrikal

Neha Thethi is an Information Security Analyst at BH Consulting (www.bhconsulting.ie).

The derived credential: delivering digital security to a mobile world

by Dr. Chris Edwards

With cyberattacks, hacks and data breaches on the rise, this article explores new methods to securely access data in an increasingly mobile economy.

Mobile usage has accelerated rapidly, and has completely changed in nature over the last few years. 60% of Internet access now comes from a mobile device – a figure that is likely to increase as we as a society become more mobile.

It's not just in our social lives. Businesses are now having to implement robust BYOD policies to cope with their employees' desire to access corporate networks and data straight from their own device – be it on site or when working remotely. It is essential that mobile access does not risk compromising required security levels for access to organizational resources.

For many years, the US Federal Government's personal identity verification (PIV) program for smart card authentication has been a cornerstone of secure physical and virtual access to resources. In order to evolve this requirement to incorporate mobile device access, the National Institute of Standards and Technology (NIST) has defined the use of a "derived credential" on mobile devices. For federal government agencies and trusted contractors, this can be used to provide secure access to corporate systems, services and data from smartphones, tablets and laptops. The derived credential ensures that access meets the appropriate required level of authentication, allowing the federal workforce to become both mobile and secure.

Smart cards and the challenge with mobile

PIV cards were implemented to improve the security of US government resources and facilities in the wake of the 9/11 terrorist attacks. Simultaneously, the Department of Defense was instigating a similar program, dubbed the Common Access Card (CAC). Over the years, the two standards have gradually converged to the extent that CAC and PIV now share a significant number of content containers and provide a largely interoperable "card edge" programming interface.

When CAC and PIV are combined with other related deployments - such as the Transportation Worker Identification Credential - there are well in excess of 10 million technically compatible smart cards currently in use by the federal government for its employees and contractors.

The smart card form factor is very convenient in many respects. It fits neatly into your wallet, can operate in contact or contactless mode, and is highly standardized, thus offering very good levels of interoperability.

The recent increase in mobility, however, has challenged the traditional smart card system. Enterprise-grade laptops typically include smart card readers, and desktop computers can be connected to external readers. Mobile devices, on the other hand, have no integrated card readers, so smart card authentication isn't an easy option.

Needless to say, there have been several attempts to provide external card readers for mobile phones, but issues such as battery life and the inconvenience of carrying another device in addition to the phone have meant the technologies never took off.

The challenge for developers was finding a way to put the credential directly into the phone or tablet, while still maintaining an acceptable level of security for the private cryptographic keys that are relied upon for authentication, signing and encryption.

As it was clear that mobile credentials would not be able to fully replace smart cards for some time, a solution based on "derived credentials" (PIV-D) was proposed in the government's revised FIPS 201-2 standard, with detailed guidance to be provided in the NIST special publication SP800-157.

THE RECENT INCREASE IN MOBILITY HAS CHALLENGED THE TRADITIONAL SMART CARD SYSTEM

Mobile in use

The ability to read encrypted emails when away from a desktop computer has been of the utmost importance for some time, so secure email was historically the primary application considered for mobile use. However, with more and more businesses demanding the ability to allow employees to work remotely with full access to secure corporate resources, packages of complete and secure cloud services are now emerging as the most important requirement.

Operating systems such as BlackBerry OS7 and Windows Mobile include a shared cryptographic service layer – a standardized programming interface through which any app can access credentials delivered to the device. Apple iOS and Android, on the other hand, do not provide a device-wide comprehensive cryptographic layer for apps. For example, certificates and keys installed using Safari on an iPhone cannot be used directly by your own apps – only by the "native" apps such as the Safari browser and the default mail app. Another challenge with iOS and Android is that there is no secondary authentication to the keychain and therefore once the phone is unlocked no further authentication is needed for access.

For enhanced security, private keys can be stored in hardware "secure elements" (SEs) embedded within the device. An SE is capable of holding keys in a non-exportable form, with cryptographic functions such as signing and encryption being performed within the SE. There are a wide variety of SEs available in phones and tablets, such as the UICC (aka SIM), TPM, secure microSD and embedded SEs that support NFC. Many of the Android-based devices on the market today support a Trusted Execution Environment (TEE), which can also provide key storage with a "trusted user interface" for PIN entry.

Derived credentials in use

The "formal" definition of a derived PIV credential is purely an authentication certificate. Extensions are permitted to allow signing and encryption certificates to be implemented, too. However, for any of these credentials to be of real use and to be widely adopted, they must be made available to work easily with apps on an employee’s mobile device.

With the wide range of cryptographic key storage devices now available – most of which support different app programming interfaces – a readily available library of programs for apps is now needed to operate across a range of mobile devices as transparently as possible. Once you add the widely requested additional features such as signing, encryption, physical access, and verifiable flash badges, the consumption of mobile credentials becomes even more challenging for app vendors.

As with any credentialing environment, a secure, policy-enforcing lifecycle management system is vital for mobile security. In the case of PIV-D, the standard describes specific business processes for the two supported levels of assurance that must be followed by any compliant solution. Such a solution must have strong authentication for operators and full audit capabilities to allow rapid, secure access to administrative functions.

One major advantage of PIV-D for users is that they are using what is effectively an "always on" connected device. This means that certificate renewals and updates can be performed without needing to attend a specific location; an Internet connection to a trusted system is all that is required.

THE MOBILE MARKET CONTINUES TO EVOLVE RAPIDLY, WITH AN INCREASING NUMBER OF OPTIONS FOR THE STORAGE AND PROCESSING OF CRYPTOGRAPHIC DATA.

Smarter access

The use of derived credentials for PIV presents the opportunity for greatly enhanced security, access and usability of protected resources from mobile devices.

The NIST special publication SP800-157, in conjunction with the FIPS 201-2 standard, provides the framework for highly practical solutions to the issues that employees and contractors encounter on a regular basis – issues that must be addressed before a workforce that needs access to sensitive and secure data can become fully mobile.

The mobile market continues to evolve rapidly, with an increasing number of options for the storage and processing of cryptographic data.

Using a vendor-neutral library to access these credentials that is capable of working equally well with card readers, hardware secure elements, Trusted Execution Environments and numerous flavors of software credential stores is therefore an extremely worthwhile investment. When compared to the alternative – a workforce that is either mobile or secure, but not both – it is clear that the time for such interoperability of credentials should be at the forefront of enterprise technology and security priorities list.

Dr. Chris Edwards is the CTO at Intercede (www.intercede.com). Chris was responsible for the initial design of Intercede's MyID product and retains overall responsibility for the architecture and use of technology within it. He has over 30 years’ senior level experience within the IT industry, 12 of them within the security sector. Chris was instrumental in making MyID the first electronic personalization system to achieve FIPS 201 accreditation as part of the US HSPD-12 PIV Approved Products Scheme, and has substantial experience of working on both US and UK government security projects.

iOS spyware used by Pawn Storm cyber spies

Trend Micro researchers have unearthed two variants of a spyware specially designed for targeting devices running iOS, and at least one of them can be installed on non-jailbroken devices. The malware is used by the attackers behind Pawn Storm, a recently discovered but long-standing cyber-espionage operation that has in the past targeted media companies, military attachés, staff at the Ministry of Defense in France, staff of the US State Department, personnel of US defense contractor ACADEMI (formerly Blackwater), and many more military and government targets.

"We believe the iOS malware gets installed on already compromised systems, and it is very similar to next stage SEDNIT malware we have found for Microsoft Windows' systems," they shared. "We found two malicious iOS applications in Operation Pawn Storm. One is called XAgent (detected as IOS_XAGENT.A) and the other one uses the name of a legitimate iOS game, MadCap (detected as IOS_ XAGENT.B). After analysis, we concluded that both are applications related to SEDNIT."

While XAgent is aimed at collecting text messages, the contents of the contact list, pictures, geo-location data, a list of installed apps and processes, information about the Wi-Fi status and can perform voice recording, MadCap is focused on audio recording. Another difference is that MadCap can only be installed on jailbroken devices. It's also interesting to note that XAgent works flawlessly on iOS7, and easily achieves stealth and persistence, while on iOS8 its presence can be detected by the visible icon, and the malicious app can't restart automatically once it has been closed. The researchers believe that this shows that the spyware was created before iOS8 was released in September 2014.

"The exact methods of installing these malware is unknown," they shared. "We have seen one instance wherein a lure involving XAgent simply says 'Tap Here to Install the Application.' The app uses Apple's ad hoc provisioning, which is a standard distribution method of Apple for iOS App developers."

New Android Trojan fakes device shut down, spies on users

A new Android Trojan that tricks users into believing they have shut their device down while it continues working, and is able to silently make calls, send messages, take photos and perform many other tasks, has been discovered and analyzed by AVG researchers. They dubbed it, and AVG's security solutions detect it as PowerOffHijack.

PowerOffHijack has been discovered in China, where it has already infected over 10,000 devices. It is apparently being propagated via third-party online app stores, but the researchers haven't mentioned what apps it masquerades as.

The Trojan is capable of infecting Android versions below v5.0 (Lollipop).

"After pressing the power button, you will see the real shutdown animation, and the phone appears off. Although the screen is black, it is still on," the researchers explained.

That's because the malware, after having previously obtained root access, is capable of injecting the system_server process that hooks the mWindowManagerFuncs object, and ultimately prevents the mWindowManagerFuncs.shutdown function to do its job, which is to first shut down radio service and then invoke the power manager service to turn the power off.

After keeping the power button pressed long enough to initiate the shut down procedure, the victims are presented with a fake pop-up that asks confirmation of the process, and see a fake shut down animation. The malware and the phone will continued working, but the screen will be black.

VirusTotal sets up huge AV whitelist to minimize false positives

One of the worst things that can happen to a software developer, and especially if they are a small firm or a single individual, is for their program to be falsely detected as malicious.

But these false positives can also be an unwelcome hindrance to many others, as end-users begin to wonder whether they should continue using the program (or their security solution prevents them from doing so), IT support teams get flooded with users' requests saying there's a problem with the software, and AV makers' reputation takes a hit.

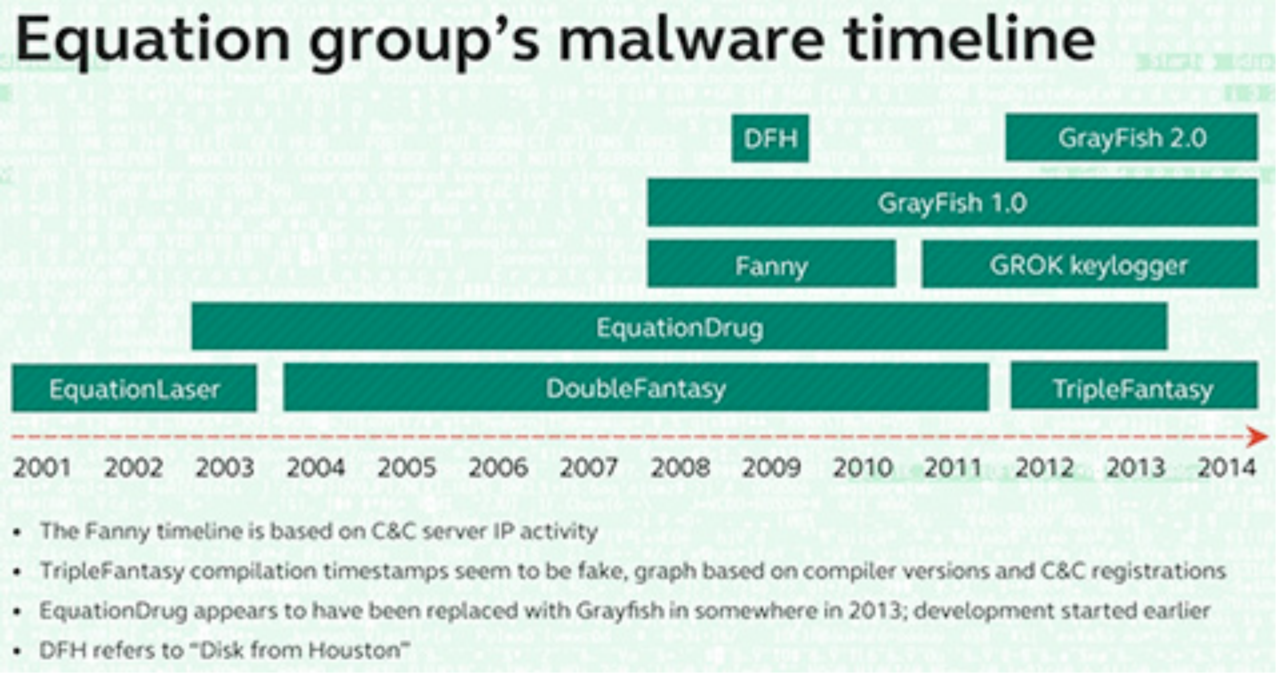
"Nowadays antivirus vendors are increasingly required to become more proactive, this includes developing generic signatures and heuristic flags, which very often leads to mistaken detections in an effort to have a more secure user-base," VirusTotal software engineer Emiliano Martinez explained the origin of the problem in a recent blog post, in which he also announced a new project that aims to minimize - if not remove altogether - this problem.

VirusTotal essentially wants to create a huge AV whitelist, and is asking software developers to share the files in their software catalogue.

"These files are then marked accordingly at VirusTotal and whenever an antivirus solution (mistakenly) detects them, we notify the pertinent vendor, allowing them to quickly correct the false positive," he shared. "Additionally, when files get distributed to antivirus vendors, they are tagged so that potential erroneous flags can be ignored, preventing a snowball effect with detection ratios."

Microsoft is the first company that took up their offer, and so far over 6000 false positives have been fixed.

Other software developers are invited to contribute to the project, but developers of potentially unwanted applications and adware need not apply.


Equation group's malware timeline

- The Fanny timeline is based on C&C server IP activity
- TripleFantasy compilation timestamps seem to be fake, graph based on compiler versions and C&C registrations
- EquationDrug appears to have been replaced with Grayfish in somewhere in 2013; development started earlier
- DFH refers to "Disk from Houston"

Equation Group: Cyber espionage, compromising HDD firmware, sophisticated malware

For several years, the Kaspersky Lab Global Research and Analysis Team (GReAT) has been monitoring more than 60 advanced threat actors responsible for cyber-attacks worldwide.

They've discovered the Equation Group, a threat actor that has been active for almost twenty years.

According to Kaspersky Lab researchers, the group uses tools that are very complicated and expensive to develop, in order to infect victims, retrieve data, hide activity, and utilize classic spying techniques to deliver malicious payloads to the victims.

To infect their victims, the group uses an arsenal of Trojans including the following that have been named by Kaspersky Lab: EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny and GrayFish. Without a doubt there will be other Trojans in existence.

Hardware

GReAT has been able to recover two modules which allow reprogramming of the hard drive firmware of more than a dozen of the popular HDD brands. By reprogramming the hard drive firmware, the group achieves two purposes:

1. A level of persistence that helps to survive disk formatting and OS reinstallation. If the malware gets into the firmware, it is available to "resurrect" itself forever. It may prevent the deletion of a certain disk sector or substitute it with a malicious one during system boot.

"Another dangerous thing is that once the hard drive gets infected with this malicious payload, it is impossible to scan its firmware. To put it simply: for most hard drives there are functions to write into the hardware firmware area, but there are no functions to read it back. It means that we are practically blind, and cannot detect hard drives that have been infected by this malware" – warns Costin Raiu, Director of the Global Research and Analysis Team at Kaspersky Lab.

2. The ability to create an invisible, persistent area hidden inside the hard drive. It is used to save exfiltrated information which can be later retrieved by the attackers.

Also, in some cases it may help the group to crack the encryption: "Taking into account the fact that their GrayFish implant is active from the very boot of the system, they have the ability to capture the encryption password and save it into this hidden area," explains Costin Raiu.

THE EQUATION GROUP USES A C&C INFRASTRUCTURE THAT INCLUDES MORE THAN 300 DOMAINS AND MORE THAN 100 SERVERS.

Fanny worm

The Fanny worm stands out from all the attacks performed by the Equation group. Its main purpose was to map air-gapped networks, in other words – to understand the topology of a network that cannot be reached, and to execute commands to those isolated systems. For this, it used a USB-based command and control mechanism which allowed the attackers to pass data back and forth from air-gapped networks.

In particular, an infected USB stick with a hidden storage area was used to collect basic system information from a computer not connected to the Internet and to send it to the C&C when the USB stick was plugged into a computer infected by Fanny and having an Internet connection. If the attackers wanted to run commands on the air-gapped networks, they could save these commands in the hidden area of the USB stick. When the stick was plugged into the air-gapped computer, Fanny recognized the commands and executed them.

Malware delivery

The attackers used universal methods to infect targets: not only through the web, but also in the physical world. For that they used an interdiction technique – intercepting physical goods and replacing them with Trojanized versions. One such example involved targeting participants at a scientific conference in Houston: upon returning home, some of the participants received a copy of the conference materials on a CD-ROM which was then used to install the group's DoubleFantasy implant into the target's machine. The exact method by which these CDs were interdicted is unknown.

There are solid links indicating that the Equation group has interacted with groups, such as the Stuxnet and Flame operators – generally from a position of superiority. The Equation group had access to zero-days before they were used by Stuxnet and Flame, and at some point they shared exploits with others. For example, in 2008 Fanny used two zero-days which were introduced into Stuxnet in June 2009 and March 2010. One of those zero-days in Stuxnet was actually a Flame module that exploits the same vulnerability and which was taken straight from the Flame platform and built into Stuxnet.

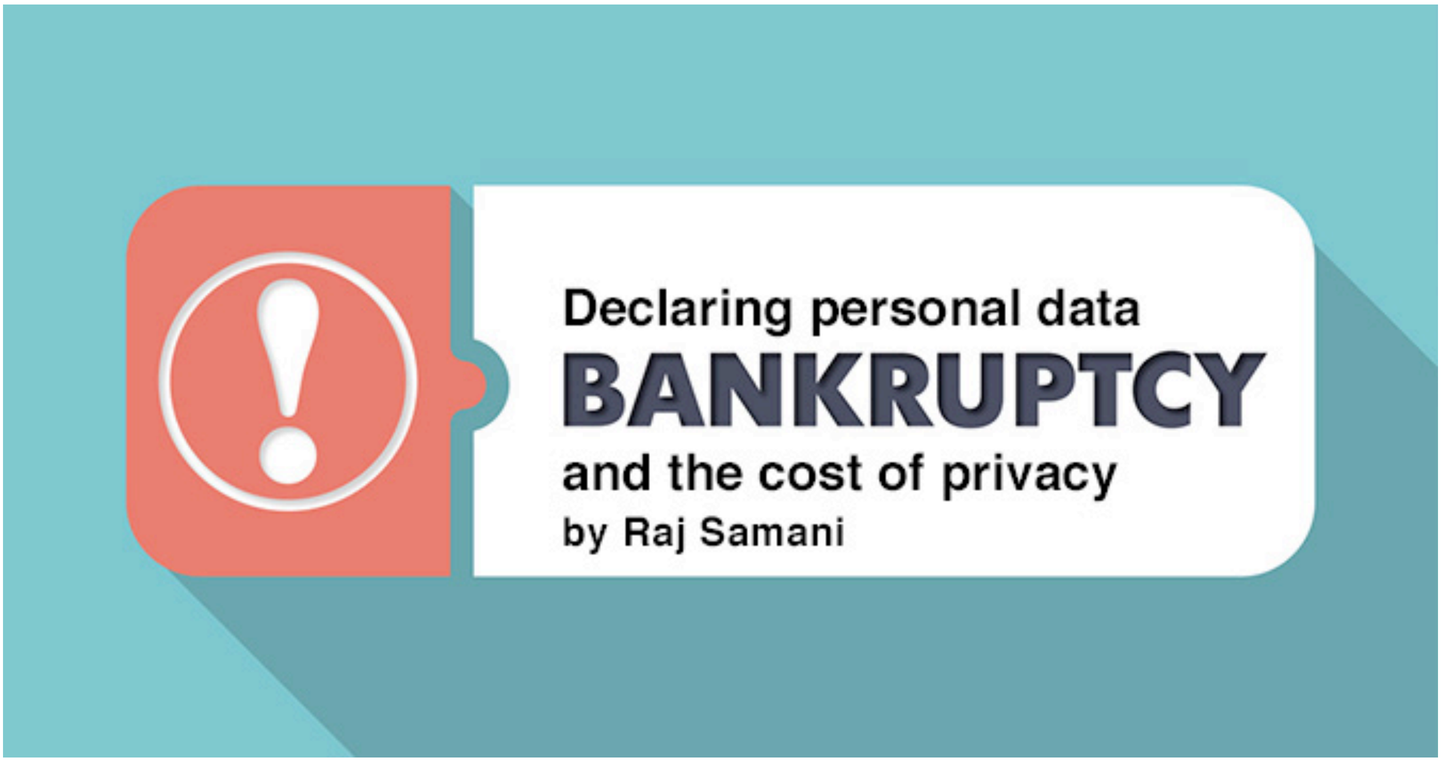
The Equation group uses a C&C infrastructure that includes more than 300 domains and more than 100 servers. The servers are hosted in multiple countries, including the US, UK, Italy, Germany, Netherlands, Panama, Costa Rica, Malaysia, Colombia and Czech Republic. Kaspersky Lab is currently sinkholing a couple dozen of the 300 C&C servers.

Since 2001, the Equation group has been busy infecting thousands, or perhaps even tens of thousands of victims in more than 30 countries worldwide, covering the following sectors: Government and diplomatic institutions, Telecommunications, Aerospace, Energy, Nuclear research, Oil and Gas, Military, Nanotechnology, Islamic activists and scholars, Mass media, Transportation, Financial institutions and companies developing encryption technologies.

Kaspersky Lab observed seven exploits used by the Equation group in their malware. At least four of these were used as zero-days. In addition to this, the use of unknown exploits was observed, possibly zero-day, against Firefox 17, as used in the Tor browser.

During the infection stage, the group has the ability to use ten exploits in a chain. However Kaspersky Lab's experts observed that no more than three are used: if the first one is not successful, they try with another one, and then with the third one. If all three exploits fail, they don't infect the system.

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



Declaring personal data BANKRUPTCY and the cost of privacy

by Raj Samani

In the digital economy, your data profile has value, but judging from what I watched happen recently in a London shopping mall, a lot of us give it away for free.

At the Westfield shopping center in Shepherd's Bush, a long line of Britons waited to surrender valuable personal information – demographic details, shopping habits, brand preferences, and more – in exchange for a free bar of chocolate. Really. How did the collector, a prominent British retailer, intend to use this bounty? None of the data donors I observed seemed to care. Not one paused to read the posted privacy disclosure statement.

That could turn out to be one costly chocolate treat.

We're a society in conflict. On one hand there's outrage over government surveillance programs and wholesale data breaches. 28% of the online population claims to use tools to disguise their identity or location. 61% of Americans say personal rights and freedoms command higher priority than anti-terror measures.

On the other hand, so many trade their identities away for a pittance, or even for nothing – valuing them, wrongly, at zero.

Why are they so ready to surrender their privacy to commercial interests? Especially when their trust is betrayed so regularly due to security lapses, with such damning publicity for retailers, banks, and more usual suspects? A lot of us voluntarily declare personal data bankruptcy. It's a big mistake.

What's personal data bankruptcy? It's when you declare your personal profile worthless. You want to know how often I go to the movies? What features I like in a new car? What magazines I read? Anyone curious is going to use all that data to make money – so pay me.

Many of us carry loyalty cards. Swipe a card at the grocery checkout, for example, and get the special "club price" on bananas, or a buy-one, get-one deal on noodles. So there's a little value. But, believe me, it pales next to the value of the personal and transactional data the store compiles.

Some organizations take advantage of the consumer's perception that his or her data is worthless by actually charging to join loyalty programs. Sadly there's no shortage of takers.

When I bought movie tickets recently, the clerk asked me if I wanted to join the cinema chain's loyalty program. With free tickets as rewards, it seemed like a fair enough transaction.

Every consumer has equity in the digital data economy.

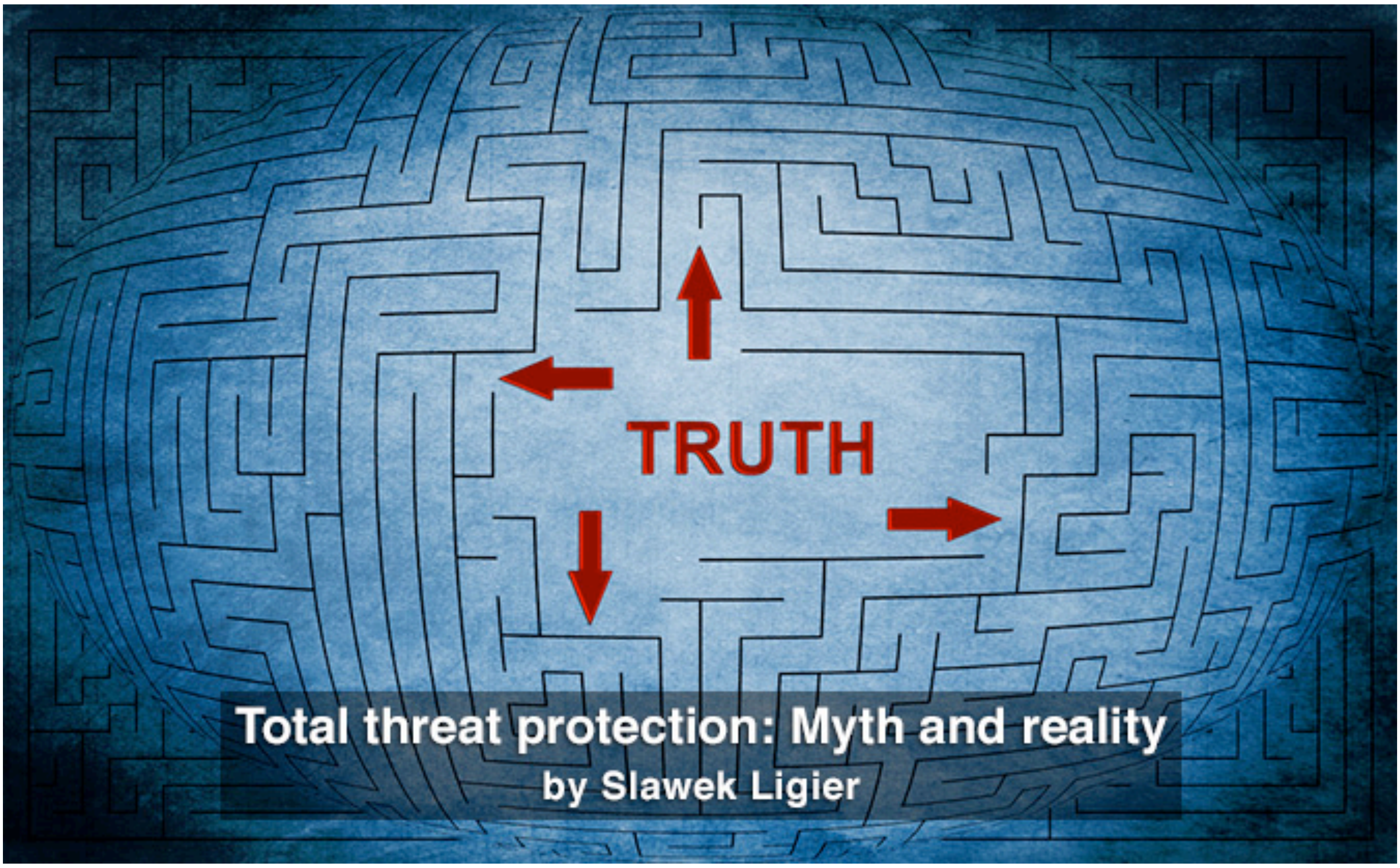
I was dumbfounded to hear there was a monetary charge for handing over my information – a charge 200,000 other moviegoers had already paid. And this is no isolated example.

Every consumer has equity in the digital data economy. Nobody's really "bankrupt." But they have to be less shy about getting what this data is worth. When we fail to assert the value of our personal data we hand its exploiters a free pass.

One alternative is to simply withdraw from the digital economy: go cash-only, pass up discounts and freebies, and share nothing. But that's not only increasingly difficult these days, it cuts you off from some real benefits of loyalty and personalized transaction systems. Better advice: be as cautious and hard-nosed about data-sharing as if you were shopping for fresh fish. Who will my data be shared with? How will it be used to shape unique offers and pricing for me? How is it protected? What are the real rewards? If the deal "stinks", do what you would do if the fish stank. Walk away.

Don't join the line for chocolate bars. Your data is prized by nearly every business you patronize. They should be lining up for you.

Raj Samani is the Vice President and CTO, EMEA, Intel Security.



Total threat protection: Myth and reality

by Slawek Ligier

Let's start by articulating clearly that there is no such thing as 100 percent protection in today's evolving threat environment. There are ways threats can be managed and mitigated, but despite what many security vendors will have you believe, there are no silver bullets.

Protecting your data is hard work that requires a combination of people, processes and security solutions. Here, we'll analyze various threats, and the techniques you can use to mitigate them. Attacks on your computing resources can come from multiple directions:

1. Compromised user accounts
2. Compromised mobile devices
3. Malicious or compromised web sites
4. Email
5. Network intrusion or denial of service
6. Remote access.

Although it is critically important to prevent intruders from penetrating your network, it is just as important to realize that if there is a will, there is a way, and your best defenses will be breached. Once that happens you might ask yourself: "How well did I protect my critical data and can I find the compromise before I lose any critical information?"

Let's start with prevention. The easiest way to gain access to a network is to have the appropriate fully authorized credentials of a user. Unfortunately, the majority of enterprises today do not use multi-factor authentication, instead relying on the old user ID/password mechanism. They fool themselves into believing that they have a high level of security by requiring complex passwords (i.e. XYZ123!@#) and rotating them every couple of months.

The result is that the users have a hard time remembering passwords, so they write them down or frequently resort to using password reset mechanisms. Increased calls to help desks force companies to cut costs by providing online password recovery, which is often the easiest way for the attacker to gain the aforementioned credentials.

Multi-factor authentication makes it much more difficult to compromise user accounts. In addition to a user ID and password, a user needs to present security clearance information only they could have – a One Time Password (OTP) generated on their mobile phone or a dedicated device, plus a PKI certificate stored on their smart card, or a biometric identification. Multi-factor authentication makes it much more difficult for unwanted users to gain access to your resources since they need to discover both the user's login ID and password, and have the second credential as well – mobile phone, smart card, or live fingerprint.

Deployment of multi-factor authentication would also allow you to reduce password complexity and eliminate the need for frequent password rotation. Passwords needed to access cash at the bank ATM use a simple 4-digit number; these are particularly effective as they do not change. This is because ATM systems rely on multi-factor authentication – you need your bank card in addition to the PIN, and this provides a relatively high level of security.

Unfortunately most companies using multi-factor authentication within the enterprise do not reduce password complexity. Done correctly, we could eliminate unnecessary calls or easy-to-bypass password reset mechanisms, thus further strengthening our defenses.

TODAY'S USERS EXPECT TO BE ABLE TO ACCESS CORPORATE RESOURCES FROM A VARIETY OF DEVICES, INCLUDING THEIR OWN

Today's users expect to be able to access corporate resources from a variety of devices, including their own. Companies need to embrace BYOD and try to manage it. Our goal should be to identify all devices accessing our network and allow only known devices to have access.

Devices that are granted access to the network should be registered and managed by the Mobile Device Management (MDM) system. MDM solutions allow us to enforce certain corporate policies such as minimum password requirements, device locking, geo tracking when the device is lost, and wiping when it is compromised.

Once a known user is rightfully inside our corporate network, we need to ensure they do not infect the network by downloading malicious software from the web or by opening innocuous-looking (but malicious) attachments sent via email.

Dedicated web filters are able to detect users' attempts to visit risky web sites, download malicious software, or use file-sharing applications. It could be educational for the system administrator to learn about the variety of cloud-based tools used in the average corporate environment.

When CIOs are asked in surveys for the number of cloud-based solutions used, the answer is around a dozen. The reality is that the scan of the typical corporate network shows hundreds. Often we find more than dozen file sync and share applications being actively used, and some of them are hosted in countries with widespread disregard for information security.

Additionally, good web filters have the capability of detecting communication methods used by malware already inside the organization, quarantining affected users and devices, and offering ways to remediate the infection.

Email is a frequently targeted attack vector (e.g. the Target hack was traced back to a phishing email). Many of the highly publicized breaches in the last few years started with email delivering malware or directing the recipient to a site hosting it. Once the malware is inside the network, it can be very difficult to detect and remove. Both incoming and outgoing email needs to be scanned for spam, malware, and confidential data leakage.

COMPANIES NEED TO EMBRACE BYOD AND TRY TO MANAGE IT

Despite the hype surrounding the need for breach acceptance, we cannot leave the perimeter unprotected. Modern firewalls can do an effective job of protecting the enterprise against denial of service or brute force attacks. They give administrators good visibility into the network traffic and provide an opportunity to segment the most critical parts of the network.

Best-of-breed solutions go beyond port monitoring and offer the ability to block specific applications and report on the applications being used by employees.

Do you know how many rogue file sync and share applications are in use in your organization? How many of them have policies specifying that any data stored in the cloud belongs to them? How many store the data in geographic locations where you might never want your data stored in?

Finally, Web Application Firewalls (WAFs) can help you secure your web sites against typical attacks. Although OWASP Top 10 vulnerabilities have been widely known for many years, developers allow SQL Injections, Cross-Site Scripting, and other attacks to succeed every day.

While it is important to conduct regular penetration testing of your Internet-facing applications and fix all vulnerabilities, it is a good practice to set up a WAF to be in front of your web server, just in case someone introduces a simple problem before it is detected by your testing.

DO YOU KNOW HOW MANY ROGUE FILE SYNC AND SHARE APPLICATIONS ARE IN USE IN YOUR ORGANIZATION?

At the beginning of the article I stated that there is no such thing as 100 percent guaranteed protection. Despite our best efforts, solutions fail and intruders win from time to time. Once that happens, it is important to mitigate the damage.

Two things are important to remember – speed of detection and protecting your most valuable data. Detection relies on analyzing traffic within your network and monitoring any egress points. In order to be effective, intruders need to take the data they have interest in outside of your network. Malware needs to communicate with command and control servers.

This communication can be detected, precautions can be taken, and alarms can be put in place, enabling IT to take appropriate actions.

It is important to be proactive and make sure your most valuable data is appropriately protected. Proper use of encryption technologies could limit the damage done to your organization. The weakest point of any encryption technology is the storage and management of keys, as well as applications that have access to those keys.

Proper design of the cryptographic solution would ensure that access to keys is tightly controlled and keys are generated and stored using secure Hardware Security Modules (HSMs).

There is no such thing as complete security. But by taking a holistic view of all threat vectors and providing adequate protection against each and every one of them, we can minimize the chances of becoming front-page news.

Slawek Ligier is the Vice President of Product Development at Barracuda (www.barracuda.com), where he fights spam, assuring that inappropriate data does not leak outside of the corporation and that users can safely browse the Internet. Prior to Barracuda, Mr. Ligier was a CTO at SafeNet protecting end user identities and assuring trust on the internet by providing solutions enabling safe key storage and encryption of critical data driving today's commerce. As a VP of Engineering at VeriSign and Symantec he was managing development of systems enabling development of trust in cyberspace.

INTERPOL *WORLD* 2015

14 - 16 APRIL 2015

Sands Expo & Convention Centre, Singapore

PLAN YOUR VISIT NOW

CYBERSECURITY

BORDER MANAGEMENT

SAFE CITIES

SUPPLY CHAIN SECURITY

YOUR PARTNERSHIP PLATFORM

INTERPOL *World* Public-Private Partnership

- Game-Changing catalyst of innovation to address global security challenges

YOUR SOURCING & BUSINESS PLATFORM

INTERPOL *World* Expo

- 250 exhibitors from over 25 countries
- Be the first to view new and innovative technologies

YOUR KNOWLEDGE & NETWORKING PLATFORM

INTERPOL *World* Congress

- Launchpad of co-created innovative solutions with leading private-sector security solutions providers

EARLY BIRD ENDS 27 FEB 2015

(LIMITED SEATS ONLY!)

YOUR BUSINESS AND NETWORKING ENGINE

Register online now at www.interpol-world.com

Event Owner

INTERPOL

Supported By

MINISTRY OF HOME AFFAIRS

SINGAPORE EXHIBITION & CONVENTION BUREAU

Supporting Knowledge Partner

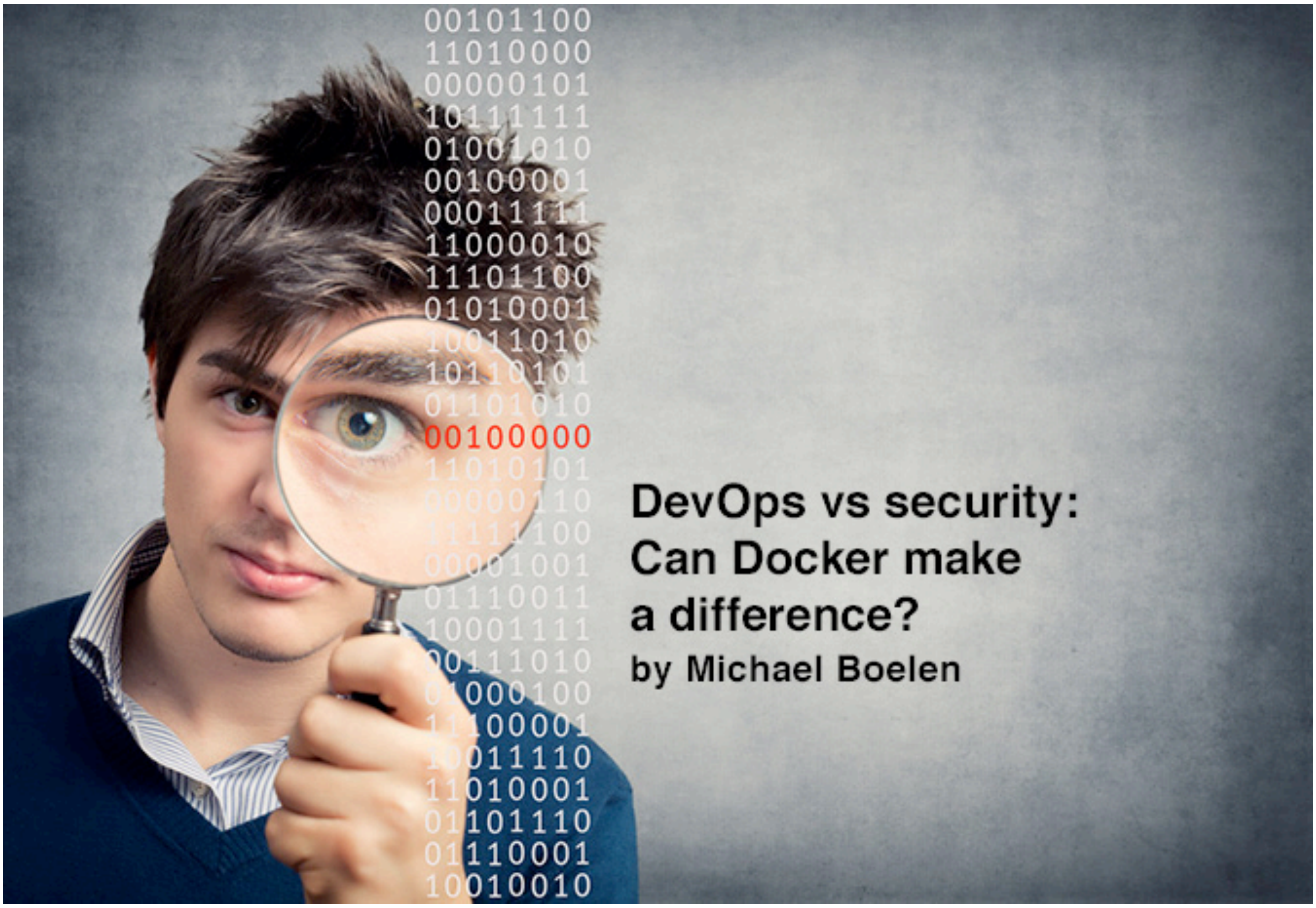
FROST & SULLIVAN

Held In

YourSingapore

Managed By

mp



DevOps vs security: Can Docker make a difference?

by Michael Boelen

One of the pioneers in the world of DevOps is Docker, Inc. Known for its toolkit around Linux container technology, they propel the evolution and world-wide promotion of this technology. But with great achievements and interest comes a lot of pressure. Competing products are popping up, fueling a battle for features, pricing and customers. Unfortunately, for security professionals like us, the many security lessons from the past seem to be forgotten. We might be end up battling the same issues as before.

In the last few years, the DevOps movement gained a lot of momentum. One of the reasons might be the need for companies to be more “agile”. This includes releasing high-quality software faster and more often, but at the same time keeping costs as low as possible.

While the benefits of DevOps are great, when it comes to the "DevOps role", there is still confusion for most people, especially as the definition is not that well-defined. Those who were previously just sysadmins or developers suddenly find themselves doing work from both worlds. And let’s be honest, it is close to impossible to be an expert in multiple areas, or keeping up with all the new developments.

Do we have a problem?

It is especially hard for auditors and security professionals to keep up with these new technologies. We simply do not have enough hours per week to extensively dive into each new technology. When technology is then also limited to one platform, we have to make a choice and specialize in one area.

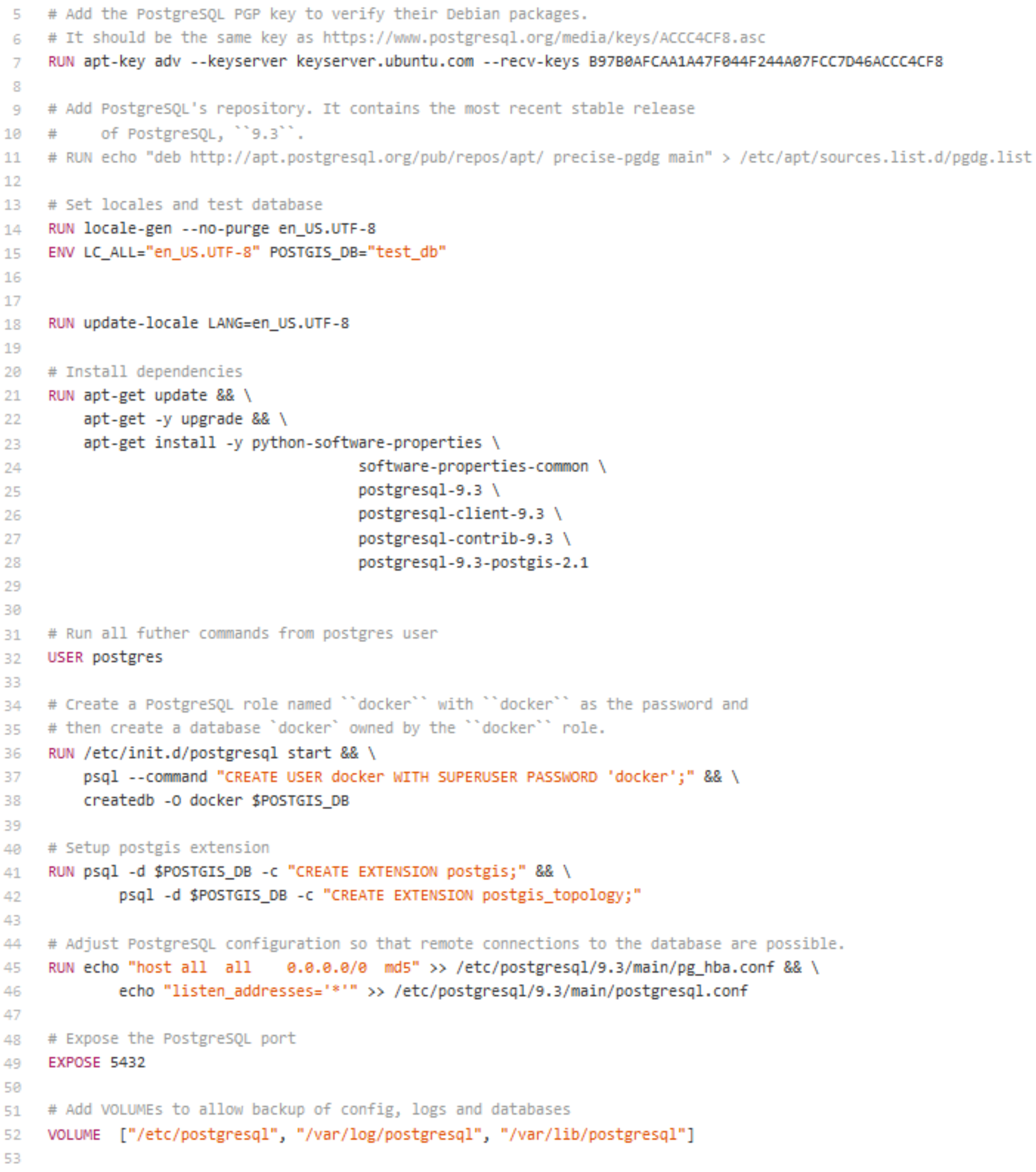
Even developers and admins who already used Docker might be confused by all available parameters. What’s worse, their number seems to increase with every new Docker release. It’s great to see SELinux support, but didn’t we all turn that off on our host system? With the existing time pressure in our work, new features are usually skipped.

This is especially true if they take a lot of time to test, deploy and monitor. We all know that security features are not usually simple and easy to deploy without extensive testing.

Docker and security

In the last few releases of Docker, the company showed that security is something you cannot simply skip. Some vulnerabilities were patched, and several new security features were introduced. Examples include allowing a limited set of capabilities and the usage of MAC frameworks. By looking at these new options, we can get a glimpse of what is already possible, and where the technology is still immature. Being a DevOps gets easier due to container technology, and at the same time more complicated as well.

Well documented Docker file:



```
# Add the PostgreSQL PGP key to verify their Debian packages.
# It should be the same key as https://www.postgresql.org/media/keys/ACCC4CF8.asc
RUN apt-key adv --keyserver keyserver.ubuntu.com --recv-keys B97B0AFCAA1A47F044F244A07FCC7D46ACCC4CF8

# Add PostgreSQL's repository. It contains the most recent stable release
#     of PostgreSQL, ``9.3``.
# RUN echo "deb http://apt.postgresql.org/pub/repos/apt/ precise-pgdg main" > /etc/apt/sources.list.d/pgdg.list

# Set locales and test database
RUN locale-gen --no-purge en_US.UTF-8
ENV LC_ALL="en_US.UTF-8" POSTGIS_DB="test_db"


RUN update-locale LANG=en_US.UTF-8

# Install dependencies
RUN apt-get update && \
    apt-get -y upgrade && \
    apt-get install -y python-software-properties \
                               software-properties-common \
                               postgresql-9.3 \
                               postgresql-client-9.3 \
                               postgresql-contrib-9.3 \
                               postgresql-9.3-postgis-2.1


# Run all futher commands from postgres user
USER postgres

# Create a PostgreSQL role named ``docker`` with ``docker`` as the password and
# then create a database `docker` owned by the ``docker`` role.
RUN /etc/init.d/postgresql start && \
    psql --command "CREATE USER docker WITH SUPERUSER PASSWORD 'docker';" && \
    createdb -O docker $POSTGIS_DB

# Setup postgis extension
RUN psql -d $POSTGIS_DB -c "CREATE EXTENSION postgis;" && \
        psql -d $POSTGIS_DB -c "CREATE EXTENSION postgis_topology;"

# Adjust PostgreSQL configuration so that remote connections to the database are possible.
RUN echo "host all  all    0.0.0.0/0  md5" >> /etc/postgresql/9.3/main/pg_hba.conf && \
        echo "listen_addresses='*'" >> /etc/postgresql/9.3/main/postgresql.conf

# Expose the PostgreSQL port
EXPOSE 5432

# Add VOLUMEs to allow backup of config, logs and databases
VOLUME  ["/etc/postgresql", "/var/log/postgresql", "/var/lib/postgresql"]

```

Containers do not contain

“Containers do not contain” is a commonly heard phrase. The current issue with containers is that they do not fully isolate - yet. One of the main reasons is that one important namespace is missing, the one dealing with users and groups. For example, gaining “root access” within the container means you get similar privileges on the host system itself. From there, it’s a small step to a compromise of the security of the whole machine.

Another reason why containers are not fully isolated is the use of keyrings, which store crypto keys. This instrument can’t yet see the difference between UID 80 in one container from another user with the same ID. Due to these constraints, we should still treat containers similar to how we treat a normal host system. For example, running services under the context of the root user was always considered a bad practice. When using containers, this practice should still be considered harmful.

Namespaces

Namespaces separate several internals of the Linux kernel, which allows it to create different “views” of what a system looks like. This way multiple environments can run on a single kernel, each with its own processes, users, network routing and mounts. It is like a virtual machine, except that containers are a single process. This reduces a lot of overhead and provides flexibility when packaging up software. Together with control groups (cgroups for short), the kernel can control processes. With cgroups the priority and resources can be controlled. While namespaces separate one big area into smaller ones, cgroups ensure that all areas behave.

Namespace complexity

Docker is actually waiting for the user namespaces to be finished, so it can leverage all its functions and get one step closer to full containment. The first few developments regarding user namespaces are finished and available. For example, the usage of subordinate users and groups is already possible. This function helps the host system map users (and groups) within each container to different users on the host itself. For example, user ID 1000 within the container might be user ID 101000 on the host system. The functionality is definitely much more complex that it looks at first sight.

One restriction was the common 16 bits limit for user IDs, limiting it to only 65535. Maybe this restriction is the easiest part to solve. A little bit more time goes into the adjusting of common userland and helper tools, to deal with the mapping of users. Examples include tools to create, modify or delete users (useradd, usermod, userdel), helper tools (newuidmap, newgidmap) and the usage of new configuration files like /etc/subuid and /etc/subgid. What looks like an easy extension in one file, turns out to affect a lot more files in the end.

Build, ship and run?

Most things in IT start in the building phase. In Docker’s case, you might want to consider spending a little bit more time in the phase before it: preparation.

Before building things, you will benefit from a clear strategy. This starts with how you want to divide applications, and what makes a container actually a container. Right now the consensus seems to be a unit, which has one primary function (e.g. be a database server, or provide a web application). Whatever you choose, ensure that there is a definition in place within your organization. From there start building containers according to that strategy.

Building

The building process is one of the most interesting parts. This is when images get built, which will be used for running new containers. At this stage security awareness and implementation depends completely on the skillset of the builder.

Unfortunately, developers usually have a lower urgency to do things the secure way than most system administrators. While the developer focuses more on “get it running”, the system administrator cares more about system stability.

The Dockerfile

Docker build files, usually with the name Dockerfile, are small scripts to guide the building process. They instruct the docker binary how to create an image, and what commands to execute.

The first thing is defining the base image from which the container will be build. Usually defining the maintainer is next, followed up by the installing of packages. If you mean to create, tune or analyze a Dockerfile, it is important to know these basic commands to determine what the container is actually doing. While the commands might have very self-explanatory names, there are subtleties you need to know about. Simply copying, pasting and adjusting an existing Dockerfile will not always give the results you seek.

Command	Function
ADD	Copy archives, downloads or data into the image.
CMD	Define default command to run (usually the service).
COPY	Copy data into the image.
ENV	Define an environment variable.
EXPOSE	Make a port available for incoming traffic to the container.
FROM	Define the base image, which contains a minimal operating system.
MAINTAINER	Maintainer of the image.
RUN	Execute a command or script.
VOLUME	Make directory available (e.g. for access, backup).
WORKDIR	Change the current work directory.

Best practices

Docker provides extensive documentation regarding the build process, including a best practices document (https://docs.docker.com/articles/dockerfile_best-practices/).

After analyzing hundreds of build files (Dockerfiles), we can conclude that many builders definitely do not follow these best practices. Issues vary from skipping simple optimization steps when installing software components to using "chmod 777" on data directories.

If you are using Docker within your organization, analyzing build files will definitely give an idea about the best practices applied within this area. Since we are talking about DevOps and automation, the open source auditing tool Lynis (https://github.com/CISOfy/Lynis/) can help you to check for some of the best practices in your Dockerfile.

Steering the ship

Even with lacking security awareness or missing security features, not all hope is lost. Docker provides a few helpful features:

- SELinux/AppApparmor support - Limit the resources which can be accessed by a specific process
- Capabilities support - Limit the maximum level of functions (or "roles") a process can achieve within the container
- Seccomp support - Allow/disallow what system calls can be used by processes
- docker exec - No more SSH in containers for just management.

We can additionally use iptables to limit the network traffic streams even further. On the host system, you might apply technologies like GRSEC and PaX, followed by other generic system hardening practices.

Conclusion

When we look at the world of vessels and containers, it becomes clear that container technology is not very mature. When we look at the security level specifically, there is even more room for improvement. At least Docker gave both the technology and security awareness a boost, resulting in the first signs of a healthy ecosystem.

The existing security features definitely look promising and are worth investigating. Let's hope this article is outdated in a few years. For now, I wish you a great and safe trip.

Michael Boelen is the founder of security firm CISOfy (https://cisofy.com), specialized in security auditing solutions for the Unix, Linux and Mac OS platform. He is in particular interested in analyzing the security of systems, including new technologies like Linux containers and Docker. Some examples of his work include open source tools, like malware scanner Rootkit Hunter, and auditing tool Lynis.

Want to reach a large audience of security pros by writing for (IN)SECURE?
STOP
Send your idea to mzorz@net-security.org

Best practices for securing PoS systems

by Numaan Huq, JD Sherry

During the last 18 months, headlines have been full of news about retailers that have been hit with payment card systems compromises. This not only includes stolen credit card information from PoS (Point of Sale) registers/ terminals, but also other sensitive customer information such as addresses, dates of birth, telephone numbers, email addresses and more.

In 2013, the FBI alerted retailers about the danger of malware stealing sensitive data, and that the attacks that have happened to that point were only the tip of the iceberg. As predicted, more infections and security breaches have occurred since then.

What can organizations do to prepare for and defend themselves against these types of targeted attacks? The situation isn't hopeless, but it takes proper planning and investment in new approaches to skill development, technology implementation and innovative analysis to do it.

Payment card data theft

Stealing payment card data has become an everyday crime that yields quick monetary gains. The goal is to steal the data stored in the magnetic stripe of payment cards, clone the cards and run charges on the accounts associated with them. Criminals have been physically skimming payments cards, such as debit and credit cards, for years. Common techniques include:

- Making a rub of the card
- Rigging ATMs or gas pumps with fake panels that steal data
- Modifying store Point-of-Sale (PoS) terminals
- Using off-the-shelf hardware keyloggers on cash registers.

These techniques all require physical access to the cards or the devices used to process them, which introduces a high risk of being apprehended. Skimmers also cannot be readily mass deployed for maximum effectiveness; therefore, criminals have resorted to using malicious software to steal payment card data, primarily credit card data. The software solution provides anonymity, ease of deployment and flexibility to adjust to changing conditions.

What is PoS RAM scraping?

After the merchant swipes the credit card, data on the card temporarily resides in plain text format in the PoS software's process memory space in Random Access Memory (RAM). The magnetic stripe on the back of the credit card contains three data tracks. Credit cards use only Track 1 and 2. When the credit card is swiped, data from both tracks are read into the PoS software's process memory.

PoS RAM scraper malware retrieves a list of running processes on the infected machine, inspects each process' memory space in RAM and searches for the credit card data. Information about the credit card data format is in the public domain; it is defined in ISO/IEC 7813.

The malware scrapes the payment card data from the RAM and exfiltrates it to the cybercriminals. The stolen Track 1 and 2 data can be used to physically clone the credit card, or can be used in fraudulent "card-not-present" transactions, e.g. online purchases.

The family tree

The earliest evidence of PoS RAM scraping can be found in the Visa Data Security Alert issued on Oct. 2, 2008. At the time, cybercriminals attempted to install debugging tools on PoS systems to dump Track 1 and 2 credit card data from the RAM. PoS RAM scrapers have quickly evolved to use multiple components and exfiltration techniques, including single binaries, network, bot and kill-switch functionality, encryption and development kits.

For you to better understand this evolution, we have organized PoS RAM scraper malware families by year of discovery in the following timeline. Note: a malware variant may have existed long before it was discovered because tracking exact dates is extremely difficult.

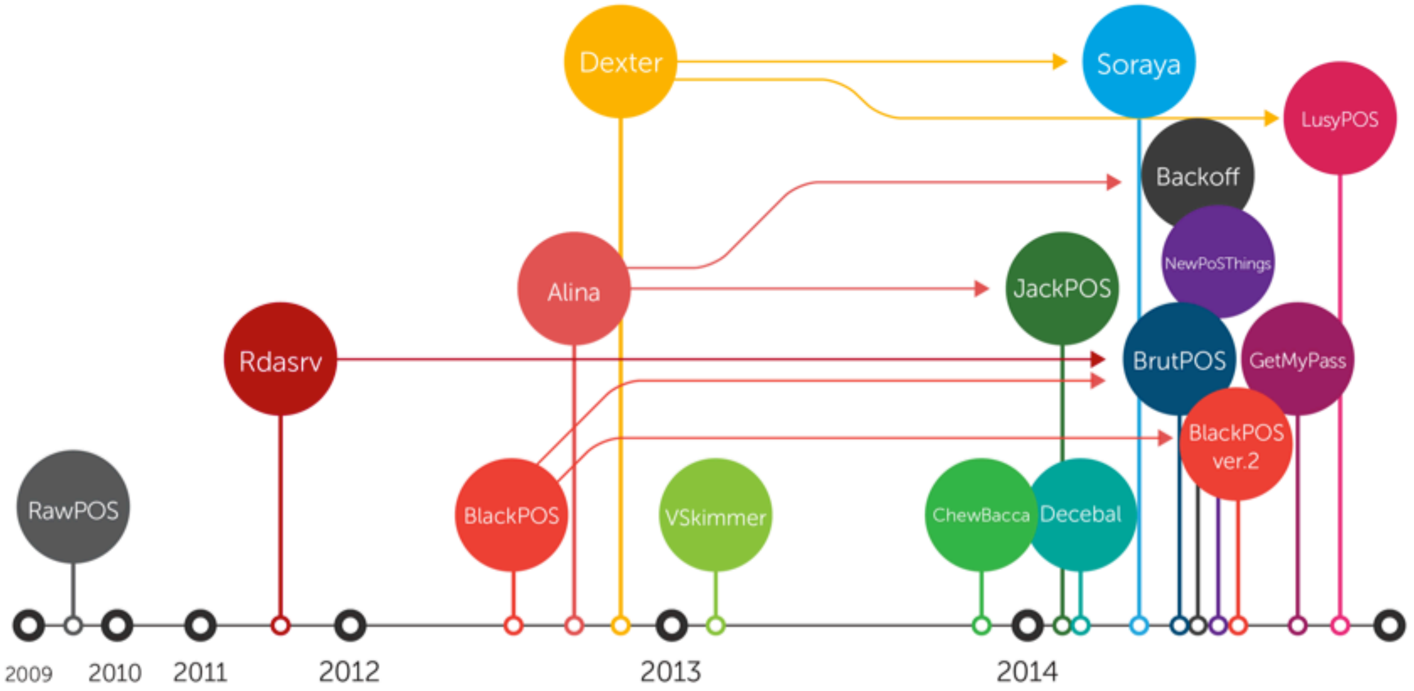


Figure 1 - PoS RAM scraper family timeline 2009-2014.

A couple of observations about the diagram:

• Seven unique PoS RAM scraper families were discovered between 2009 and 2013.
• Nine unique PoS RAM scraper families were discovered in 2014 alone.
• The arrows connecting the bubbles indicate either a direct evolution or technology reuse.

The attack chain

The key to setting up a strong defense is to understand the nature of the threat. In the case of PoS RAM scrapers, this means understanding the malware's attack chain. Through countless hours of research, security analysts have been able to observe trends and patterns on how these attacks persist and are ultimately successful.

Retailers and businesses that process credit cards are now targets, regardless of size. The most convenient place to steal credit card data is directly from the RAM of the PoS systems, where the data temporarily resides in plain text format during transaction processing. The challenge for cybercriminals is to find a reliable method to infect PoS systems. Options include:

1. **Inside jobs** – Inside jobs are the most difficult infection vector to protect against, as it involves people that businesses trust, or who can abuse privileges to commit a crime. They could be disgruntled employees seeking revenge, or unscrupulous individuals out to make some quick cash.

2. **Phishing and social engineering** – PoS RAM scrapers are never spammed out to millions of potential victims. Instead, they are sent to a chosen few targets via phishing emails with effective social engineering lures. Small businesses often use their PoS servers to browse the Internet and check email, thus making them easy targets.

3. **Vulnerability exploitation** – new software vulnerabilities are disclosed and patched every month by their respective vendors. Only a handful of these are successfully “weaponized.” Once weaponized, the vulnerabilities will be used in cyber attacks for years. Exploits successfully compromise systems because patches for the vulnerabilities have not been applied, and many PoS servers are still running operating systems that are no longer supported.

4. **PCI-DSS non-compliance abuse** – PCI-DSS refers to a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. PCI-DSS does not offer new secure technologies to protect electronic payment systems. Instead, it provides standards to build-up additional layers of security controls around existing ones. Hardening systems and networks is not a trivial task. Companies that lack expertise or resources often incorrectly configure their PoS environments, thus making them susceptible to different attacks that compromise them with malware.

5. **Targeted cyber attacks** – Some of the most successful PoS RAM scraper attacks against large businesses have been “targeted attacks.” A targeted attack can be broken down into six stages: victim reconnaissance, phishing and social engineering attack, callback, lateral movement, data collection and data exfiltration. Targeted attacks are meticulously planned and well-executed, making them difficult to detect.

Defending a businesses

PoS RAM scraper malware attacks have evolved to target any business that processes credit cards. With PCI-DSS and PA-DSS compliance requirements being tightened, security strategies can no longer be viewed as a checkmark; security is now an integral component of business operations.

Strategic security decisions

To effectively protect against PoS RAM scraper attacks, businesses must protect all aspects of their operating environment, not just the PoS systems. Attackers might gain initial entry into the corporate network using compromised credentials or via spear phishing emails, then use lateral movement to traverse the network, locate PoS systems and infect them.

Organizations need to consider many factors when making security strategy decisions, such as:

• **The size of the organization** – large organizations have complex network topologies, thousands of connected devices, multiple locations, etc. Security solutions need to be scalable and centrally managed.

• **The costs** – security solutions can become expensive, especially when the organization requires multi-tiered defenses. Businesses should also factor in costs of in-house or externally contracted IT services required to manage the deployed security solutions.

• **Multi-platform support** – many businesses support all the major OS platforms in their operating environments. Security solutions must be able to protect multiple OS platforms and provide centralized management of the protected devices.

• **BYOD** – organizations are increasingly moving toward implementing BYOD policies as a means of cutting costs and giving employees flexibility. BYOD policies introduce new challenges of securing employee owned devices that are accessing the organization's resources.

What's next

Implementation of chip and pin/EMV (Europay, Mastercard, Visa) technology, as well as that of next generation payment platforms and e-walleting capabilities will help reduce PoS attacks. However, it won't guarantee the elimination of payment attacks completely.

Retailers and financial institutions should work diligently to determine the possible failure points of their systems.

Consumers and end users will also have to adopt a shared security model by taking the necessary steps to ensure their devices are protected. As we move to a more frictionless form of payment capability, the very devices that we enable to carry out these payment transactions must be pristine. Multi-factor/ biometric capabilities should also be embraced to thwart future attacks.

Investments should be made to create rich PoS payment applications that are securely tied to our mobile devices that can leverage cheap technology to process and transmit transactions.

Spending hundreds of millions, and potentially billions, across the US to implement EMV technology is cumbersome for consumers. At the rate technology is advancing, this form of payment will quickly be outmoded.

THE FUTURE RESTS ON SOFTWARE AND NOT HARDWARE

The US must take the lead in ushering in a new transaction model. Why use a physical credit card, when NFC (Near Field Communications) and secure encrypted apps are readily available to harness the processing power of the cloud and the convenience of a mobile platform? There should be more of a demand on retailers to look ahead to where the payment model is going, not where it was.

The future rests on software and not hardware - technology should be near frictionless and become part of how we interact with the rest of our world. Hardware and physical means for conducing payments are expensive to maintain, which makes the cost prohibitive.

The FBI warned in January 2014 that we haven't seen the end of PoS breaches, and they were right. Target, PF Chang's, UPS, Home Depot; the list continues to grow. There are most likely other payment-processing organizations that have fallen victim to these type of attacks, but do not yet realize the damage.

Let's prevent a future filled with these attacks.

Let's be forward-thinking about where the market is going and invest in the right payment platform, one that we will be able to scale now and in the future.

Numaan Huq, is a member of the forward-looking threat research team, and JD Sherry is vice president, technology & solutions for Trend Micro (www.trendmicro.com).

InfoSec World Conference & Expo 2015

www.misti.com/infosecworld

Disney's Contemporary Resort, Orlando, USA / 20 March - 25 March 2015

InfoSec World 2015 will have a lineup of conference sessions, workshops and summits that address the most pressing matters in information security today. With a selection of top-rated speakers, you'll find content that is compelling, actionable and applicable to the current challenges you face at your job.

RSA Conference USA 2015

www.rsaconference.com

Moscone Center, San Francisco, USA / 20 April - 24 April 2015

RSA Conferences are the pulse point of the security industry where leading practitioners connect to protect. Here you'll meet with top industry leaders and fellow security specialists to discover how the latest advances in technology can help you meet those challenges.

HITBSecConf2015 Amsterdam

conference.hitb.org/hitbsecconf2015ams

De Beurs van Berlage, Amsterdam, The Netherlands / 26 May - 29 May 2015

This year's event will feature new training courses. Keynote speakers include Marcia Hofmann and John Matherly. To encourage the spirit of inquisitiveness and innovation, Haxpo will showcase cutting edge technology and security solutions for industry professionals alongside fun, hands-on tinkering and hacking exhibits.

Earn Up to 55 CPEs!
Top-notch training. Compelling speakers. Meaningful interactions.

Challenges faced by global network professionals

with Ken Kartsen, Senior Vice President of Federal, Intel Security

Interview by Mirko Zorz

Ken Kartsen is the Senior Vice President of Federal at Intel Security. In this interview he offers firsthand experience of the challenges facing network professionals worldwide.

Explaining security ROI and other complex IT security issues to senior management can be a daunting task for infosec professionals in large organizations.

What are some of the unique challenges encountered by those working for the government?

I think of security as much different than other functions in the enterprise. Traditionally, in such areas as enterprise resource planning (ERP), industries start out fragmented but over time there's consolidation, which in the short term can leave you without best-of-breed, but over the long haul can reduce complexity and increase ROI.

Can you imagine still having separate systems for AP, AR – or word processing, email, and spreadsheets? Of course not; organizations have long ago consolidated those functions. Today we're even seeing consolidation to cloud. Security, however, has been much more fragmented, with organizations acquiring a new technology and technology provider for each new threat or threat vector.

There has been some consolidation by major providers, but integration has been lacking, and the costs have sometimes been overbearing. Many enterprises have close to 100 security vendors.

The best security vendors strive to reduce complexity and increase ROI by integrating disparate technologies and using open standards. The best vendors should also allow third party threat information to be combined with the vendor's and customer's own threat data, then aim to distribute it in real time.

Corporations can usually offer a higher salary than the government. With rapid threat evolution and infosec staff in high demand, how will the global shortage of skilled IT security experts impact the capability of the government to offer efficient protection on every level? How can innovative technology help in this situation?

It's abundantly clear that the outsourcing of platforms and management with mechanisms such as managed services and cloud has the potential to reduce overall costs, leverage highly available resources, and return traditional personnel to making important security decisions as opposed to technically managing technologies.

Managed services and cloud reduce internal demand for highly technical skills while allowing the enterprise to focus back on their mission. They do this in a model that reduces cost expenditure on technical resources as well as the quantity needed, while increasing broad technical proficiency.

For reasons such as these, we've leveraged our traditional portfolio into a platform and consumption model conducive to allowing the enterprise to deploy technologies and capabilities in ever changing environments.

Historically we've looked at software, hardware, and appliance solutions for on premise security protection. Today's portfolio evolved to cover those traditional needs while also supporting SaaS and managed service environments, supporting the cloud and cloud providers such as AWS and Azure, and supporting hybrid cloud environments such as VMware NSX.

Not only do these solutions include endpoint, network, and management solutions, but there is also innovative technology within each of them that can assist in creating greater efficiencies for the government. For example, a next generation firewall consolidates many historic network solutions into one appliance or virtual appliance, not only reducing rack space and costs but also management capacity.

MANAGED SERVICES AND CLOUD REDUCE INTERNAL DEMAND FOR HIGHLY TECHNICAL SKILLS WHILE ALLOWING THE ENTERPRISE TO FOCUS BACK ON THEIR MISSION

With increasing pressure to go as digital as possible, what type of technology do you expect to be essential in the complex security architectures run by modern governments?

There's no doubt that complexity within enterprise environments has exponentially driven up security architecture complexity.

There's always a need to consolidate capabilities that both overlap and have the ability to integrate more seamlessly. For example, the best next generation firewalls have the ability to not just reduce the integration points by consolidating firewall, virtual private networking, intrusion protection, and content inspection, but also to include new capabilities such as application visibility and control - all in a scaled environment with huge resiliency.

We also see this with management tools, which can collapse the visibility and control all into a centralized management infrastructure, or SIEM, to not only provide seamless management but also situational awareness.

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

Who are the role models in cyberspace?

by Chase Cunningham

Those of us of who are of a certain age learned how to live our life by playing with our toys—our cars, dolls and, of course, Star Wars action figures.

We were surrounded by role models, whether they be our parents, aunts, uncles, teachers, Batman, G.I. Joe or Princess Leia, and we witnessed people dealing with the same challenges we'd face growing up in the real world. They influenced us through their positive behavior, moral compass, street smarts and courage. As kids, we emulated these role models—we created magical adventures while playing with our toys and friends. We practiced navigating our future lives using our imagination.

Who do our kids aspire to be in their digital lives?

Cyberspace isn't the Magic Kingdom. It's the Wild West—only worse, as it's a place where it's really difficult to observe people as they make choices and experience the consequences. So corporate social responsibility programs try to drive a consciousness-raising dialogue among young people to fill the void. Sadly, what they deliver is often hopelessly lame and condescending.

They miss that being an awesome role model takes serious effort—and that in the case of our digital lives, one that has to be backed by the creative vision necessary to set out and define this new frontier. This is something new—something we never experienced at their age.

Instead, we justify our efforts by claiming we only have a "limited budget" to guide kids to their future. Some just want to tick a box to show that we are "helping the children" and move on. And so kids are shown silly dogs, flying saucers, or the occasional cyber kitty—accompanied by bullet point guidance more suitable for corporate PowerPoint presentations.

Seriously, how are these going to inspire kids to want to make smart choices online?

Being a cyber role model is more than being a successful Internet entrepreneur. It's living a smart and ethical life online. It's treating people and data with respect. Sounds straightforward, no? But here's the problem: It's hard for many kids to see their parents as digital role models because their parents don't open up their online lives to their kids. In email, social media, online shopping or web surfing, parents operate in virtual isolation to their children. Our kids aren't riding sidecar as we drive our digital lives; but that's the view of the cyber world that kids need to experience. Just like daily life, it's not a fairytale; it's a place where there are real consequences.

Where are the cyber role models?

My fellow infosec colleagues, I'm here to tell you, we are the role models for all the children in our lives. We are the ones who must fill this void. We are the ones who have the power to change the direction of our kids' digital futures. Armed with our expertise and experiences, we need to live transparent digital lives, where kids can see how we make smart choices online.

How can you begin to transform yourself into a super cyber role model?

My daughters and I take online shopping trips together. Just like I know that they watch and help me while riding in the shopping cart in the grocery store or while holding my hand in a department store, they can help me shop online too, and learn how to model their digital consumer behavior.

With that in mind, here are a few pointers while shopping e-commerce sites together.

1. Check your Wi-Fi

Before we spend money on the Internet, first we always make sure to double-check our Wi-Fi connection. Bad guys have been known to set up Wi-Fi traps, where they monitor everything we send through our Internet connection in hopes of stealing our credit card numbers, passwords, names and addresses. We only shop online by connecting through our own network or using a virtual private network (VPN). If we can't use one of those systems we don't shop, we wait until we find a connection we know.

2. Did you arrive at the correct web address?

Think like a bad guy here—what's the easiest way to get you into his fake online store? One method is creating a web address that's similar to the one you are trying to visit. All they have to do is take advantage of a frequent typo or maybe use a different top level domain, like .net instead of .com. That's why we always make sure the online store we're shopping is the one we really want. Try to avoid shopping by using a search engine because search engines don't always distinguish between malicious shopping sites and the real ones.

3. Look for the lock

We never buy anything from a website that doesn't show us a locked padlock during the purchasing transaction. It's the symbol showing that an SSL (Secure Sockets Layer) is installed. SSL creates an encrypted link between your computer and a server. It allows us to securely transmit sensitive data like credit card numbers across cyberspace.

4. Read the rules

Hold on! Are you about to click the "buy" button? Did you read the rules? Online stores have all kinds of policies about returns, exchanges, and customer service. What if you need to return the gift? What can you do if the gift doesn't show up on time? What if the person who is receiving your gift needs a different size? There is no one size fits all return/exchange policy in e-commerce. Ensuring an online store's customer policies match our needs is an important part of shopping online. Once you tap "buy", often it's too late.

Be a cyber role model for your kids. Involve them in your digital life. Inspire your kids to want to be cyber smart. Because if you don't become their digital role model—chances are no one else will either.

Chase Cunningham is the CTO at CynjaTech (www.thecynja.com).

Tackling today’s authentication complexities

by Jason Hart

Once protected by the isolated confines of enterprise IT, business boundaries have been permanently warped by the juggernauts of virtualization and cloud computing. Now, both standard users and IT professionals must contend with an increasingly complex authentication environment - one in which multiple identities are using multiple endpoints in order to access multiple applications.

According to SafeNet’s 2014 Authentication Survey, only 15 percent of organizations worldwide mandate multi-factor authentication (MFA) for 90-100 percent of their employees. With over 2 million records compromised daily, the remaining vast majority of organizations are jeopardizing the confidentiality and integrity of their networks, applications and intellectual property, leaving them at the mercy of cyber thieves.

Among organizations that do embrace MFA, CISOs today can stroll down easy street, with features such as uniform security policies, central management, visibility, and transparency into their entire authentication environment. But sysadmins happen to also be tasked with putting out IT fires and maintaining and upgrading their organization’s network infrastructure, systems, and applications. That means one of the biggest tasks today is implementing identity and access management (IAM) technologies that actually make people’s jobs easier; offering reduced time spent on management and administration, along with the ability to securely adopt new technologies.

The challenge boils down to finding a way to secure multiple identities from multiple endpoints, while simultaneously allowing sysadmins to reduce their own workload. They, in turn, can allow their organization’s mobile workforce to thrive by logging in from anywhere and confidently utilizing the latest and greatest apps and platforms. One way to achieve this is to tackle the problem of password fatigue, which some organizations are working to achieve through the use of frictionless authentication methods.

A study published by the National Institute of Technology and Standards (NIST) entitled “Report: Authentication Diary Study,” found that, on average, NIST employees authenticated 23 times within a 24-hour period, with "over-authentication" requirements resulting in user frustration, aka password fatigue, as well as coping with strategies that jeopardize security down the line, such as writing down passwords.

In enterprise authentication scenarios, however, users cannot simply walk away to avoid authentication. Hence, the importance of frictionless authentication methods such as OTP, OOBA, and tokenless authentication (for example, context-based authentication), which enhance user experience and lower barriers of adoption.

How can organizations resolve password aggravation and offer users a frictionless authentication experience? Here are some guiding principles:

Secure SSO with strong authentication: This elevates the level of assurance that a user is in fact who they claim to be, and strong multi-factor authentication can be added to ESSO/federated SSO scenarios without incurring the high cost of user inconvenience.

Lower barriers for users: Remove the need to physically carry additional daily authentication props. Context-based authentication, out-of-band software tokens and phone-as-a-token options provide convenient enterprise mobility from any endpoint.

Eliminate reliance on passwords: Two-factor authentication can completely replace static passwords, eliminating password fatigue, password administration, and password vulnerabilities.

Offer self-service: Keep dependence on help desk personnel to a minimum and offer users extensive self-service functionalities, such as resetting their profile details, requesting a new token, or synching a current one.

Bringing the focus away from the end-users and back to the administrator, there are a number of other IAM functionalities that are garnering added attention:

Automated token provisioning – Both automated token provisioning and de-provisioning utilize periodic synching with existing user stores (such as AD, Oracle, SQL, Lotus, Novell, IBM, etc.) in order to effect the appropriate actions.

Autosynching and auto-provisioning – These functionalities automatically issue tokens to new users, and automatically request activation via email notification. Similarly, they also disable a user's access permissions once they are removed from the user store.

Automated user and solution management – These capabilities can provide automated alerts delivered through SMS or email, containing real-time red flag notifications on incidents that require follow up action, thus allowing management by exception. Examples include notifications to users and administrators in the event of account lockout, modification of a key configuration setting, or the absence of user enrollments by a certain date.

Group-based policies – These policy capabilities streamline the provisioning and authorization process. For example, different user groups can be assigned with different pre-authentication rules, such as time and day or IP address restrictions, application permissions, and token provisioning configurations.

Federated login – With SAML-based identity federation, solutions can extend user store identities to the cloud, enabling users to sign in to software-as-a-service (SaaS) and cloud applications with the same credentials used to log in to the corporate network. In effect, this allows for the ability to sign in only once and concurrently gain access to multiple SaaS applications.

As-a-Service delivery – Strong authentication and identity management can be delivered as-a-Service from the cloud, further lowering TCO with cloud computing efficiencies.

A solid authentication scheme can be fluid, and even transparent to users, and can provide an extensible authentication framework to cloud and enterprise applications – allowing CISOs and sysadmins to not only fulfill their duties but also drive up efficiency and innovation.

Jason Hart is the Vice President, Cloud Solutions for Identity & Data Protection, Gemalto (www.gemalto.com).