CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Wearable Tech
Smartphone Hacking
Application Hardening
Data Recovery

October 2015

MORE INSIDE!

CONTENTS

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Alex Lating
Lee Ying
Krishna Kurapati
Wes Withrow
Christian Mairoll
Patrick Kehoe
Milica Djekic
Jeff Michael
Vladimir de Ramos
Kowsik Guruswamy
Mike Cobb
Francisco Amato
Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

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

Executive Producer:
Gary S. Miliefsky, CISSP®

SmartPhones & Internet of Things, Insecure New Trojan Horses

Friends,

In this month's edition of Cyber Warnings, we wanted to share some ideas in the area of security for smart devices. Whether it's the car hacking stories you read about in the news or the internet enabled webcams turning into botnets, no matter where you turn, you hear about hackers finding more innovative places to plant their flag and call their territory.

Imagine you've just solved your company's biggest bring your own device (BYOD) dilemma, only to find ½ the employees start wearing smart watches that soon will have complete computers built within and of course wireless and cellular connectivity. Add to that some storage, input/output and downloadable malware…I mean 'trusted apps' with lots of permissions (yes, malware), you have the ultimate spying device. But unlike James Bond who used these tools on his wrist for his own benefit, you'll be the Trojan horse for hackers, cybercriminals and malware and won't even know it.

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

Now is the best time to study smartphone hacking as well as the internet of things (IoT). If you don't begin to demand of these hardware vendors, a stronger, safer, more secure device, expect them to become backdoors and botnets. To stay one step ahead of the next step, you'll need to manage the risk of these devices being allowed on corporate networks as well as their comings and their goings. Sometimes employees will complain about their employee-owned equipment becoming managed but you must inform them that without their agreement to help you secure the complete network and BYOD environment as a whole, they might inadvertently become an accomplice in cyber theft within your organization.

Customers are always deaf to the complaints of the corporate victim. They will demand and even use class action lawsuits and other means to not be responsible for your loss of their data. Be vigilant and consider IoT and BYOD a big new attack vector in your risk management equation.

To our faithful readers, Enjoy

Pierluigi Paganini

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

Who's Talking Cyber at Your Company's Grown-up Table?

By Alex Lating, Product Marketing Manager, Hexis Cyber Solutions

So hopefully I'm not the only one who used to sit at the "kids table" during big family meals. I'm not really sure when it was decided that one was old enough to make the move to the grown-up table, but when that day finally arrived… it was a big deal.

Well, the day has come at last for security professionals to take their place at the adult table. It wasn't long ago that we didn't even have cybersecurity teams, let alone someone who effectively represented them in the overall conversations of the business.

But with the breach environment we're facing, and major companies making the headlines with cyber-attack news, it's not surprising that the tides are turning.

Two organizations that are making this change in big ways are Uber and Parsons.

Uber announced earlier this week that they are quadrupling the size of their cybersecurity staff.

After an attack in the beginning of 2015 in which information on over 50,000 drivers was compromised, the company knew they needed to step up their cybersecurity game.

The taxi-ordering servicer brought on Joe Sullivan as their new CSO and as he realized the challenges he would face in ensuring that unauthorized users don't gain access to sensitive data, he knew he needed a larger team.

Sullivan made the call to grow the team from 25 people to 100 by the end of the year.

Another company making big hiring decisions on the security side is Parsons Corp., a construction and engineering company based in California.

When they needed to fill a seat on their board of directors, they made the decision to bring on a cyber pro, instead of another dude in a suit. An interesting decision considering PWC reports that 30% of boards never even talk about cybersecurity.

Here's the thing. With the skills gap for security professionals growing, organizations that prioritize building their cybersecurity and incident response teams now will benefit greatly in the long run.

In fact, the results of a recent Ponemon Institute study found that in enterprises where the executive team proactively invests in cybersecurity tools and policies, the overall cost of a data breach is reduced.

For example, having a set incident response plan can reduce the cost a business bears after a data breach by about thirteen dollars per record stolen.

Not only does it save time and resources when executives have a written policy for incidence response, it saves money too.

Breaches are inevitable. We all know that. So why wouldn't you want to put a cyber-expert at the table?

About the Author

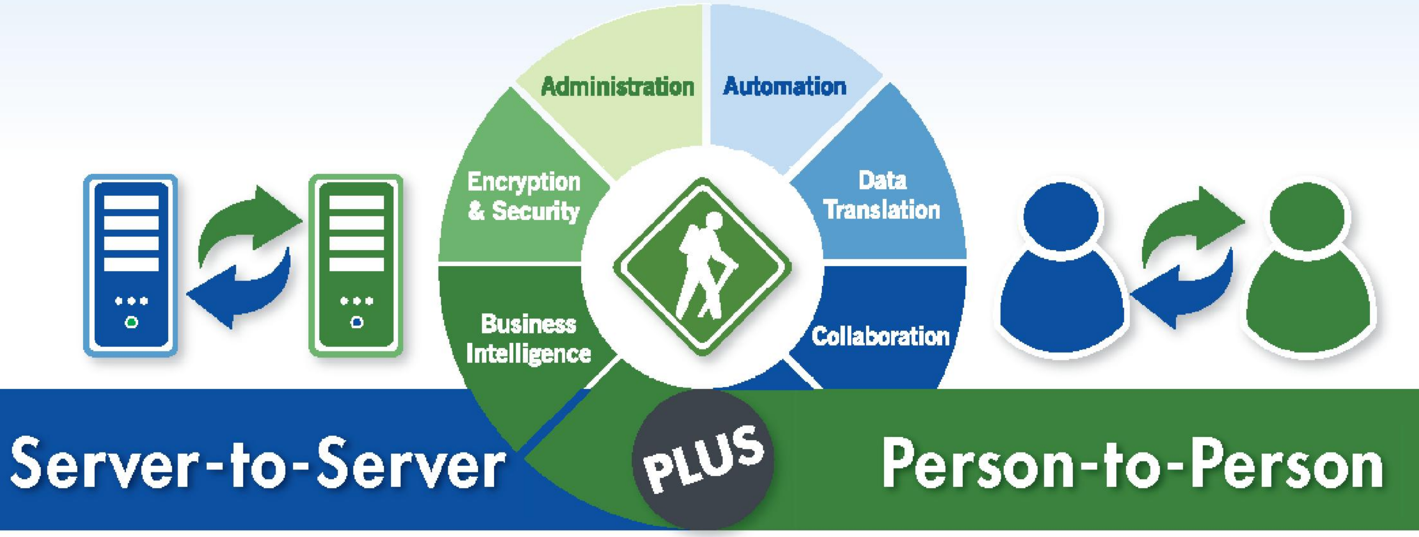
Alex Lating began working for Hexis Cyber Solutions in 2015 as the product marketing manager. Previously she has worked at Gemalto and SafeNet and is currently studying to receive her MBA from Loyola University Maryland.

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

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

Twitter: @hexis_cyber

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



Administration
Automation
Encryption & Security
Data Translation
Business Intelligence
Collaboration
Server-to-Server
PLUS
Person-to-Person

5 Things We Will Need to Do to Secure Wearable Technology

Wearable technology is certainly enjoying its moment in the spotlight. From Fitbit, Google Glass and the Apple Watch, to highly evolved adaptations tailored to those with medical requirements, computers are no longer confined to desktops, laptops, or even phones. And whether consumer-driven or needs-based, "wearables" are currently leading us in exciting new directions. But like most unprecedented developments, they inspire their share of trepidation. Concerns about security and the possibility of hacking abound, leading tech pioneers to examine a number of solutions. In terms of physical security technology has already covered this sector through products such as Pro-Vigil. For digital security here are five measures that we as a society are going to have to pursue, if we are going to be able to trust the security of the technology we wear.

1. **Optimize Design**

Smart retailers know the simple truth that people won't buy technology that isn't both convenient and modern. That's why a rush to supply products ahead of competitors while attending to said demands has left security by the wayside. Wearable smart-watches, for example, are designed to be worn nearly constantly, and therefore have few defenses if stolen or lost. In the coming years, wearable technology designers will need to design their products to hedge against any form of theft, physical or digital.

2. **Be Vigilant**

Wearable tech security starts with the wearer. If your favored form of wearable tech is linked to your phone or your personal computer, ensure that all linked devices are password-protected. Use anti-malware and antivirus software on all devices, especially if you frequently use the same wireless network. You may also wish to use a program that periodically erases internet traces, making it more difficult for untrustworthy sites to cull your information.

3. **Separate the Personal from the Professional**

In a culture that tends to look favorably upon the “constant work mode mentality”, the blurring of the line between work and home life is becoming more typical. However, while it can be unhealthy for employees to adopt a lifestyle that precludes personal time, it is just as unhealthy for the companies that these employees represent. Accessing corporate data from personal wearable devices poses a dangerous security risk, one that is compounded by the use of a home wireless network. To minimize this practice, efficiency within the workplace should be encouraged while taking one's work home should be discouraged. This facet of security should ideally be a seamless team effort between employer and employee.

4. **Adjust the Office Accordingly**

BYOD or "Bring Your Own Device" policies have become rampant in office settings, encouraging employees to provide their own personal computers and cellular devices while forgoing office-shared technology. For the sake of ease and portability, a multitude of employees have turned to wearable tech to fulfill their workplace needs, however this trend poses a threat to business security. A plethora of devices straining the capabilities of the office WiFi not only decreases overall internet speed for everyone on the network, but it also heightens the potentiality of shared viruses and malware, especially since these policies take damage control out of the hands of IT departments. To turn the tide, offices must be willing to provide in-house devices, and impose policies governing which devices can be connected to company networks, and when.

5. **Realign Expectations**

In recent years, the field of wearable technology has become a playground for creative forces and unrestrained imagination. This isn't poised to change, nor should it be; rather these forces simply need to be channeled in a direction that considers our unprecedented level of connectivity, and what that means for security. Connectivity once meant reaching an old friend via social networks, but the meaning is ever-expanding with the advent of wearable tech. Wearing a built-in GPS device on your wrist provides all the information an unscrupulous competitor needs to know about where you took a meeting, while using your wearable to pay for services digitally can leave your company credit card vulnerable. The wearer's expectations and assumptions of safety will need to be re-measured against these new standards.

About the Author

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

2015 marks the beginning of widespread Smartphone Hacking

By Krishna Kurapati, Founder and CEO of qliqSOFT

With over 3 Billion smartphones world wide in use that is expected to grow to 5.9 Billion by 2020, http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf, the smartphone has become a dominant platform of choice for computing & communication.

Unlike previous generations of cell phones that were primarily used for calls and some interesting games, the smartphone has become a computer in hand that can do everything a computer can do plus make calls.

With over 50 billion apps downloaded in last few years, it has become the platform of choice for all applications. This unprecedented rise of smartphone usage has attracted hackers to use the smartphone as a cyber criminal platform.

Apple's iPhone has had a good run in terms of security. For over eight years it's been wildly popular and yet virtually malware-free, long enough to easily earn the title of the world's most secure smartphone.

That has been recently challenged by following attacks emanating from China.

XcodeGhost attack

Heart of the iPhone security model is the process of creating apps and availability of the apps through iTunes. Virtually all the apps have to go through an approval process.

Apps are created on Xcode, the Software Development Tool provided by Apple. When an App is created, it needs to be signed by the certificate provided to the developer by Apple.

Then upload securely to iTunes for Apple’s approval. Apple does many automated checks and also manual inspections to make sure that the Apps do not violate Apple’s policies.

Hackers hit the heart of this process. Like Greeks took down Troy with Trojan horse, they have created a tainted version of Xcode, which is made available on servers for developers to download it instead of regular Xcode.

The tainted Xcode, XcodeGhost, has the ability to induce malware surreptitiously. When an iPhone user downloads app created by XcodeGhost, the app can do malicious activities from within the app. Several popular apps such as WeChat and ride sharing app are infected.

Apple discovered this and followed up quickly removed the infected apps from iTunes.

iOS Malware

Over just the last month, Chinese iPhone and iPad owners have been hit with two distinct iOS mass malware infections. Unlike previous spates of iOS-targeted malware, many of those victims hadn't jailbroken their phones to install unauthorized apps.

In at least the most recent of these two attacks, victims did have to make an almost comical series of blunders to have their phone hacked. The malware, which Palo Alto Networks called YiSpecter in its detailed writeup, tricked users into circumventing Apple's tightly controlled App Store to install a porn video player. (In some cases the hackers used local internet service providers in China, which are known to hijack traffic to insert ads on websites, to advertise the sexy video app in pop-up prompts.) If the user fell for that lure, the hackers managed to skirt Apple's App Store and install the app by using a so-called "enterprise certificate," a system that allows companies and agencies to install their own custom programs on employees' phones without Apple's signoff.

“Unteathered” Jailbreaking

Over the years, Apple has introduced features to its mobile operating system, iOS, that made jailbreaking your iPhone in order to customize and tweak your phone or tablet less appealing.

The jailbreak consists of a Windows software package that allows for an “untethered” jailbreak – meaning, your device doesn’t have to be plugged into your computer to run. The jailbreak reportedly works on iPhones, iPads, and iPod touch devices running iOS 9 through 9.0.2.

After jailbreaking, users are able to install Cydia, a framework that lets you download and install unofficial packages onto your device that allow you to run apps or make changes the iOS operating system would otherwise prevent.

Android Phones are more vulnerable to attacks from hackers since there are many ways to download and install apps from any Android Appstore. The Android install base worldwide is much larger than iPhone install base.

As more and more hackers are targeting smartphones to conduct cyber crimes, the users must be aware of potential danger to their personal information and likelihood of their phones be used to launch phishing attacks.

Users can take few essential steps to curtail cyber crimes.

1. Only download apps from Appstore or Google Play. Do not download apps from any other store unless authorized for their work.
2. Go to Settings for each app downloaded and limit the permissions. For example do not allow a Game App to access Contacts.
3. Set encryption ON
4. Set PIN/Passcode

Developers of the Apps should also be careful with Apps. It not only impacts the users but also the App developers reputation and business when their App is the one which contains malware.

1. Do not share App Developer Connect site password with many developers. Keep it controlled. Only one or two lead developers should know the password. If you can avoid it, do not share the password with contractors who you may hire to develop a module.
2. Do not download libraries that are not widely used. Make sure that the libraries that you integrate have good reputation
3. Finally do not use Software Development Tools such as Xcode and Android Development Kit from any source other than Apple or Google.

With billions of smartphones with tens of billions of App downloads, it is very hard to keep the security intact without any outbreaks of malware. As always in security, those who protect need to be always right and those who are trying to break need to be right only once.

Safe Applications

Certain applications have been developed for the purpose of safe communication without risk of hacking. For example, qliqSOFT provides Secure Texting dedicated to mobile interactions of medical professionals. qliqSOFT allows healthcare providers to close the communication loop by using mobile messaging on smartphones and tablets to communicate patient information in a HIPAA-compliant manner.

About the Author

Krishna Kurapati founder of qliqSOFT with 20 years of communications and security experience. A successful Serial Tech Entrepreneur, prior to qliqSOFT, Krishna Kurapati founded two VoIP-based companies: IPCell and Sipera. IPCell was the first VoIP switch vendor to garner several million users and it was acquired by Cisco for $240MM in funding from Silicon Valley-based Sequoia Capital, a top-tier venture capital firm and was acquired by Avaya.

Security and Compliance: A Balancing Act of Inequalities

Wes Withrow, Cybersecurity Expert for TraceSecurity

At some point in every IT security professional's career they will be asked 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 ingrained 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 historically has 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 over time that eliminates the scrambling.

Heightened Visibility Changes the Security Perception

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

To understand it more clearly, let’s first wrap some historical context around 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 the subtle nudge to the industry 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 as to why compliant and secure are not equal.

Offensive Capabilities Prove to Be 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 a 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 on businesses to secure data by both regulators and customers 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? Who is more important, PCI-DSS or GLBA? The list of questions goes on in an infinite loop.

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.

About the Author

By Wes Withrow, Cybersecurity Expert at TraceSecurity, a leader in 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 to leverage when implementing their information security program. www.tracesecurity.com

For more than 15 years, Wes has worked in IT and information security. He began his career as a systems engineer at Under Armour, the global leader in performance apparel. Wes then joined the nation's largest university affiliated research center, The Johns Hopkins University Applied Physics Laboratory, which for over 70 years has provided our nation with critical contributions in the area of national security and space. At the Applied Physics Lab, Wes served in roles that included enterprise IT operations management, systems engineering, and information security, working closely with multiple branches of the Department of Defense.

Wes leveraged the diversity of his expertise to become the CIO at a business and technology consulting group responsible for providing managed IT services to industries that include legal, finance, oil and gas, healthcare, and education. Wes obtained a Master of Science in Information Systems from The Johns Hopkins University and a Bachelor of Science in Computer Science from Davis and Elkins College.

He holds 13 industry certifications, which include the CISSP, CompTIA Security+, CompTIA Network+, Six Sigma, and HIPAA from both The Johns Hopkins University School of Medicine and the U.S Department of the Navy and has first-hand experience responding to state-sponsored cyber attacks.

Wes Withrow

504-239-3585

wesw@tracesecurity.com

www.tracesecurity.com

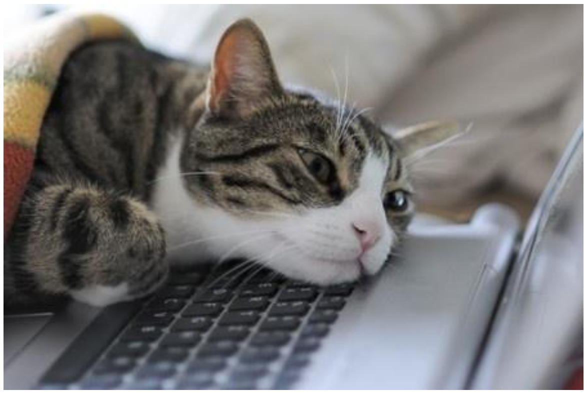
Keeping your kids safe online? Follow these 5 tips

It's a nightmare come true – your (grand)children are sitting at the dinner table or lying around in the living room, vulnerable to unknown threats. Your mind spins as you wonder, what in the world are my children looking at? Are they downloading explicit content, or planning to meet with sexual predators?

And most importantly: isn't our home the one place my kids should be safe?

What you don't know can hurt your child

Your children are glued to the screen at all kinds of odd hours, and you're completely unsure of what they're up to. It can drive you crazy just trying to imagine what's reaching them through that blue light.



It's hard to understand why young people are so completely obsessed with the Internet – but for them it's much more than a useful tool. It's where they socialize, learn, play, and express themselves. For many of these digital natives, the Internet is where a large portion of their lives will play out.

While it's important to give children the space to grow and explore, it's also important to cultivate awareness of the following threats to their safety:

Malware and privacy threats

Kids and teens love torrenting and file sharing, and often their peers will tell them about all the latest games, movies, and music that they just must have. Kids might know how to acquire all of this media, but they also might be downloading malware along with it.

This kind of behavior can also get them heavily monitored by companies that are likely working on behalf of copyright enforcers. While they might not care about their privacy now, a bad choice now could be something that haunts them in the years to come.

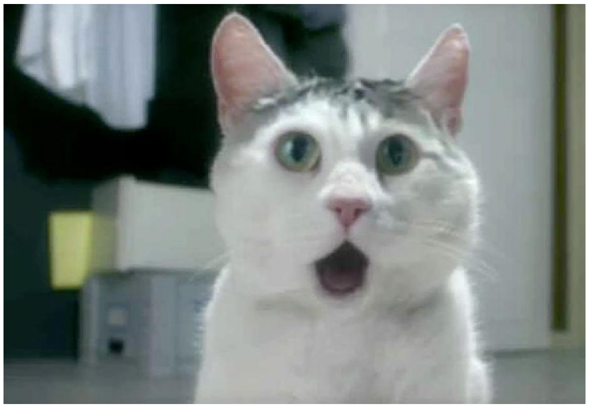
Video game addiction

If your children are gamers, you're probably used to strange shouting and compulsive clicking coming from their rooms. It may be hard to believe, but those silly online games could actually rule your children's life – people have even died from their inability to put the controller down.

Video game addiction is a real and serious problem. Like addictions to drugs and alcohol, video game addiction can get in the way of a person's ability to live a normal and meaningful life. It can lead to obesity, hallucinations, irritability, and depression. It may seem like your kids' preference for video games over socializing and school is not so out of the ordinary, but if your children are spending upwards of five hours a day gaming, it can negatively affect them on much deeper levels.

Predators on social media

It's easy to see then why kids love social media so much – they can instantly connect with their peers, and collect "likes" and "upvotes" for their thoughts and pictures. Unfortunately, a predator can also leverage these same social media features to lure in your pride and joy.



"OMG cat" (source: mashable.com)

They can even create convincing fake profiles to trick your kids, as Youtuber Coby Persin shows in his social media experiment in this video, where he convinces young girls (with the permission of their parents) to meet him in person with a fake Facebook profile. While this hoax was roused to teach the teens a lesson, it's heartbreaking to realize how easily they could have fallen victim to a real predator.

Illegal activities and pornography

Unfortunately, when kids have questions they have the Internet at their fingertips. 93% of boys and 62% of girls have been exposed to pornography before the age of 18. This could influence them to be promiscuous at a young age, or even share nude pictures or sexually-charged messages online.

And if that isn't scary enough, thanks to the growing black market on the darknet, kids can now buy drugs online. Drug trafficking on the internet is very convenient for people who otherwise might not have those kind of connections. Even if your children aren't surfing the underbelly of the internet, they can easily learn about drugs, how to use them, and where to acquire them by conducting a quick Google search.

How to stop cyber threats in their tracks

With all of the risks and dangers out there, it can be tempting to ban your children from Internet access entirely. You did have other things on your mind than the Internet when you were a child, and you turned out okay, right? Why can't they just use encyclopedias when they have to look something up? What's so bad about using the phone to call up their friends?

Unfortunately, this kind of paranoia will not prepare them for their technology-driven future, where they'll have to conduct themselves as adults daily. Luckily, you don't have to keep the keyboard under lock and key to ensure the safety of your children.

Here are the top 5 ways to keep your kids safe from Internet threats:

1. Start a conversation with your child

It's important to have an open dialogue about risks online with your kids. Bring up the conversation in relevant ways, tying in the topic to current events or TV specials. Try to get your children to express their opinions, that way you can start an ongoing dialogue about Internet safety.

Talk to your kids about other topics too. If they feel a strong social bond with you, they may turn to the computer less to cure their boredom or loneliness. Having an open line of communication can inspire your children to approach you for advice and guidance.

Serious cat (source imgfave.com)

2. Create rules and guidelines

If your children are old enough, you do not want to have to control every little thing they do. After all, you don't spend all day at school with them dictating their choices. But similar to limiting what toys you buy them, you can create boundaries surrounding new software and video game downloads. Question their motives when they ask to download:

- File-sharing software
- Torrenting software
- Anonymous browsers
- Films or music that have yet to be released

This suggests they may be interested in doing something illegal or risky. Additionally, set Internet use limits if you feel that your kids spends too much time online. Create rules surrounding social media, and how much of their personal information they are allowed to share on it.

3. Monitor your child online

Young children should never be on the Internet without adult supervision. Use these tips when sitting down with your child to explore the web:

- Set all search engines to safesearch. You can even do this on sites such as Youtube, which is a favorite among kids. Scroll down to the bottom of the page and click the safety box.
- Limit the apps and media on your phone and tablet. If your children use your devices, only have what you wouldn't mind your child accidentally coming across. If you have a Windows phone, the Kid's Corner feature can help you limit access to certain content on your device

(and prevent your little sweetheart from deleting all of your vacation photos). Just go to Settings under App list to set it up.

- Consider purchasing a child-friendly tablet. These often come with pre-installed parental controls and settings, and some even allow you to restrict access to entertainment apps so that you can get your children to focus on education.
- If your kids use a Windows 10 device, take advantage of the family features which allow you to set time and access limits. Your children will need Microsoft accounts, so be sure to familiarize yourself with the ways you can optimize privacy settings on Windows 10.

When your kids grow older, it may be wise to let this ritual go and give them your trust unless they abuse it, since most teenagers will know how to clear browser histories anyway. Cyber safety educator Leonie Smith recommends that you perform spot checks for young teens, meaning that you check in with their computer and phone use randomly. However, these checks should not be conducted in secret – you should be very clear with your children on your monitoring practices to preserve trust.

4. Use the right tools

The right tools are integral to making sure that your children don't download a harmful trojan in the event that they do come across an untrustworthy site. Investing in a quality antimalware solution can prevent nasty, system-compromising infections.

Additionally, there are parental control softwares that can help you monitor your children's activities. These applications range from blocking inappropriate websites to sending you reports on your little one's computing habits. While it may be worthwhile to consider investing in these tools, relying on them exclusively could prove to be ineffective. Kids learn how to bypass these systems, especially if they are browser add-ons.

Some trusted parental control tools include:

K9 Web Protection

A simple software that focuses primarily on blocking inappropriate websites and ads. It has a "timeout" feature that can be activated if K9 had to block too many sites in a set period of time.

Zoodles Kids Mode

Looking to protect your children while they're on your tablet or phone? Zoodles Kids Mode is an app that limits your children's surfing to a curated assortment of games, educational content, and videos. It's a good option for those times when you can't monitor your kids as carefully as you would like.

Qustodio

A comprehensive, cross-device software for those who want to receive more detailed reports about what their kids are doing. Qustodio allows you to set up separate accounts, making it a good choice for those with multiple children with different safety needs.

5. Know the signs of addiction

If your children act out when you ask them to turn off the computer and they seem withdrawn from other activities, the computer may be a problem. Know the signs of addiction, and look out for things like:

- Irritability
- Dishonesty
- Secretive behavior
- Isolation
- Back pain
- Strained vision
- Anxiety
- Poor academic performance

If you're concerned that your children may be suffering from video game or computer addiction, seek professional help for a proper evaluation. With all of the risks and dangers out there, it can be tempting to ban your kids from Internet access entirely. Unfortunately, this will not prepare them for the online world when they are adults. Addressing the issue of online safety now will help them develop the digital smarts they need to excel in an increasingly technology-driven world – all while keeping them out of harm's way.

Don't forget, it's good to log off the web as a family every now and again. Teach your kids the value of the great outdoors and real-life human contact – they might even update their status about it later!

What do you do to protect your young ones online? Do you have any tips for other parents?

Have a great, safety-conscious day!

About the Author

Christian is the founder and a CEO of Emsisoft, a New Zealand anti-malware company. For CDM, his aim is to educate our readers with essential security knowledge, especially in understanding and stopping new and innovative malware.

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

ISNR

INTERNATIONAL EXHIBITION FOR
NATIONAL SECURITY & RESILIENCE

15-17 MARCH 2016
ADNEC, ABU DHABI, U.A.E
www.isnrabudhabi.com

CROWD MANAGEMENT

THE FUTURE OF POLICING

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

DISASTER PREVENTION

INFOSECURITY

PLANNING FOR FUTURE GROWTH AND SUCCESS IN 2016

18,000 ATTENDEES

200+ GOVERNMENT BUYERS AND DELEGATIONS

500+ EXHIBITORS

90+ PARTICIPATING COUNTRIES

SOLUTIONS FOR AN UNPREDICTABLE WORLD

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

BOOK YOUR STAND TODAY!

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

Platinum sponsor

TRA

Featuring

infosecurity MIDDLE EAST

EMDI

Co-located events

FFME FIRE FIGHTING MIDDLE EAST

OSHME

Organised by

Reed Exhibitions

abudhabipolice
@abudhabipolice
theabudhabipolice
moiuae

What approach to application hardening is right for your organization?

There's no shortage of readily available hacker tools and techniques and stories in the news about mobile app hacks for both the iOS and Android platforms.

Fortunately, security solutions providers have responded swiftly and there are many approaches that one can leverage to harden an app that is "out in the wild."

For those of you who may not be familiar with the term, hardening is a key step at the end of any secure software development lifecycle process which:

- Confirms that the app is running as designed at runtime
- Thwarts hackers' efforts to reverse engineer the app back to source code

Which hardening approach is right for your app? To the uninformed purchaser, simple obfuscators are attractive because they are low in cost, require little training and are quick to implement. However, given the sophistication of today's hackers, it is important for app developers to look beyond the surface and take a more strategic approach to choosing an application hardening solution.

Below are four key factors that IT Security professionals should consider when evaluating application hardening solutions:

#1: Value of your applications

A key factor to consider is the level of investment your company is making in an app in terms of R&D and maintenance costs.

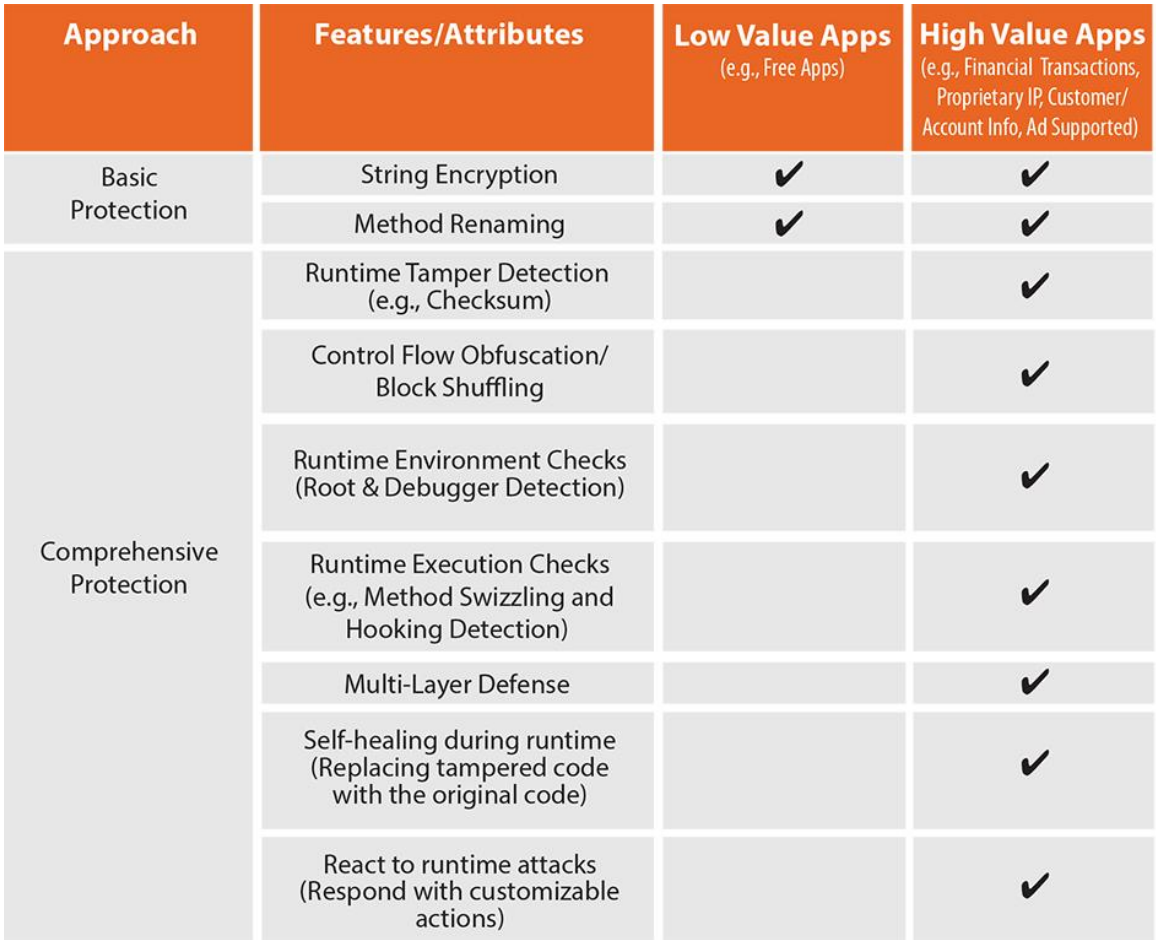
- If valuable *proprietary intellectual property* such as algorithms or monetizable content is embedded within the app, you should consider the potential revenue loss to your company if the app is successfully hacked.
- If the app processes sensitive information such as *financial transactions, account information or authorization credentials*, you should consider the potential loss of revenue through fraud and potential collateral damage that could occur if the app is hacked or Trojanized. Collateral damage may include penalties for non-compliance with regulations, expenditures on security upgrades, and even costs associated with crisis management communication campaigns to manage adverse publicity and restore brand value.

There is a prevalent belief that encryption and basic obfuscation techniques in and of themselves are adequate measures to protect apps against hacking. String encryption and variable renaming form a beneficial security layer, but they are inadequate when used in isolation.

Also, it is important to understand that not all obfuscation and encryption tools are created equal. Obfuscation is often confused with simple method renaming techniques and basic string obfuscation technologies, which can be quickly broken and easily reversed. Further, any encryption wrapper that applies the same measures of protection across all the apps it secures can be easily broken by determined hackers. Remember that once a wrapper technology is broken, *every* application secured by that vendor will be compromised.

See chart 1 below for recommended protection techniques for Low and High Value apps

Chart 1: Recommended Protection Techniques



Approach	Features/Attributes	Low Value Apps (e.g., Free Apps)	High Value Apps (e.g., Financial Transactions, Proprietary IP, Customer/ Account Info, Ad Supported)
Basic Protection	String Encryption	✔	✔
	Method Renaming	✔	✔
Comprehensive Protection	Runtime Tamper Detection (e.g., Checksum)		✔
	Control Flow Obfuscation/ Block Shuffling		✔
	Runtime Environment Checks (Root & Debugger Detection)		✔
	Runtime Execution Checks (e.g., Method Swizzling and Hooking Detection)		✔
	Multi-Layer Defense		✔
	Self-healing during runtime (Replacing tampered code with the original code)		✔
	React to runtime attacks (Respond with customizable actions)		✔

#2: Scale and Sophistication of Attacks Your Apps Will Likely Face

Minimal protections against counterfeiting and repackaging are built into the app distribution ecosystem -- including measures such as:

- Detection of jailbreak or root conditions that enable side-loading of applications, many of which are Trojanized.
- Monetization libraries to confirm that only legitimate applications are downloaded through an app store and that they are correctly purchased or licensed. However, these libraries can and are often breached by cybercriminals.

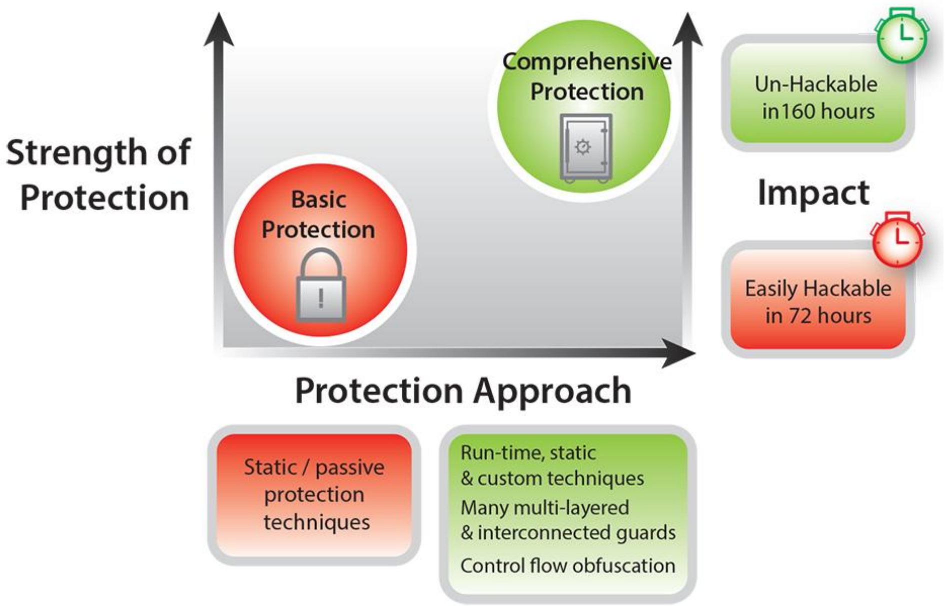
- Audit processes to validate that only legitimate and harmless apps are placed in the app store. Audit mechanisms to block illegitimate apps from distribution to users are far from perfect, as seen by recent iOS malware, including XcodeGhost.

Consequently, it is important to determine the scale and sophistication of attacks that you anticipate for your applications, and validate that the security solution you rely on is capable of meeting the challenge. For small-scale developers with free- or ad-supported apps, typically basic application protection will suffice, even though ad revenue may be subverted through Trojanization.

In contrast, for business-critical enterprise applications, it is safe to assume that an organized army of hackers will be actively looking for ways to subvert your app as quickly and as comprehensively as possible. Since such attacks are designed to be covert, it can take weeks or even months until evidence of a successful hack surfaces. For that reason, measures of defense against attacks have to be complemented by measures of detection and reaction. For example, deeply instrumenting an app to detect attempted attacks and react with functions such as "phone home" can provide long-lasting and durable protection.

Consider the recent benchmarking study that analyzed an Android Java mobile payment application that was hardened with a comprehensive protection solution against the same application with a Basic Java protection solution. Key findings from the study appear in the chart below:

Chart 2: Strength of Protection of Basic and Comprehensive Hardening Techniques


Strength of Protection
Comprehensive Protection
Basic Protection
Un-Hackable in160 hours
Impact
Easily Hackable in 72 hours
Protection Approach
Static / passive protection techniques
Run-time, static & custom techniques
Many multi-layered & interconnected guards
Control flow obfuscation

Attacks that systemically compromise the underlying libraries an app relies on are the fastest growing class of attacks – and presently the most dangerous.

This makes it imperative that high value apps are able to verify the pristine nature of their entire execution environment before unlocking sensitive functionality.

Obfuscation solutions that focus solely on variable renaming or string encryption can deter static reverse engineering but are not able to protect against the full spectrum of high-intensity attempts to compromise the app.

#3: Agility and Portability

The portable device ecosystem, spanning smartphones and tablets and wearable devices, is among the fastest growing and fastest evolving. In stark contrast to the PC ecosystem -- which is dominated by only a few chipset and operating system combinations, the portable ecosystem is a combinatorial nightmare of chipsets, OSs, programming technologies and hardware functionality.

Because it is likely that mobile platforms will continue to evolve at their current breakneck and unpredictable pace, choosing a solid security partner with a history of innovation- that can keep pace with evolving ecosystems- is crucial. Additionally, selecting a security tool that is designed for cross-platform portability and extensibility will go a long way in helping you adapt to new platforms that become available.

#4: Overhead and Performance Impact

Memory footprint, power consumption and performance are important considerations in portable devices, where resources are limited and battery life is precious.

All security technology will impose an additional memory footprint in storage and at run-time. It will also impose process overhead in terms of programming effort, compilation complexity and run-time execution characteristics.

That said, more sophisticated application hardening solutions can offer a stronger trade-off between performance impact and protection strength relative to free- or low-cost solutions.

For example, brute-force simple obfuscation can quickly cause memory bloat and diminish execution speed, while basic check summing can adversely impact run-time performance while retaining single points of protection failure.

When apps are deployed to millions or billions of users, and/or where transaction volumes are expected to be high, it is crucial that the security solution chosen be as robust and reliable as your own app code.

Obfuscating sections of the code that are sensitive to performance degradation, such as computation-intensive functions or graphics rendering routines, has an impact on runtime performance. It's paramount to *choose a protection solution that offers tunable performance vs. security tradeoff measures*, and provides developers better control on size and performance of their code.

The rise of mobile computing and soaring app usage has companies of every size and caliber scrambling to keep up. With customer loyalty and revenues at stake, developers are scrambling to release cutting-edge apps with little thought for long-term security considerations.

In these conditions, it is tempting to treat code hardening as a checkbox and select the cheapest, most readily downloadable tool to do the job – but let the buyer beware.

If you take the time to assess the value of your applications and the available options, you'll realize that if you have a high value app and focus solely on cost, you are likely to be "penny wise and pound foolish."

About the Author

Patrick Kehoe joined Arxan in January 2014 as Chief Marketing Officer. Mr. Kehoe has over twenty years of experience building and managing sales and marketing capabilities for software, hardware, and service providers in the High Tech industry. Over the past three years, he held leadership positions at Siemens Enterprise Communications (SEN) – a global provider of communications software and services. Most recently he was responsible for North American marketing and partner business, where he oversaw the development of the strategic plan and drove Market Awareness, Pipeline Generation, and Sales results.

Previously, he managed SEN's Global Marketing Strategy, Intelligence, and Operations. Prior to SEN, Mr. Kehoe held positions at Booz Allen Hamilton and MarketBridge, a Sales and Marketing Professional Services Firm, where his clients included: IBM, SAP, Symantec, and VeriSign. Among other areas of focus, he was responsible for market expansion, new product marketing, digital marketing, and social media. Mr. Kehoe has a track record of success in North America, Europe, South America, and Asia, and has spoken at conferences and corporate events on a variety of sales and marketing topics. He holds a degree in Computer Science from Vanderbilt University and a MBA from the Darden Graduate School of Business, University of Virginia.

EXHIBIT IN 2016

SSS
Saudi Safety & Security
2016

Saudi Arabia's leading security, fire and safety exhibition

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

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

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

2015 PARTICIPANTS

ASIS International, وزارة الصحة Ministry of Health, UL, iosh, Saudi Electricity Company, National Water Company, Saline Water Conversion Corporation, Saudi Aramco, سابك sabic, KBR, EMERSON, DUPONT, K·A·CARE

ARMADA, Petrofac, GEXCON, 2N, 3M, ABLOY, TSS, AFI, amanco, ADINA, Aventura, avigilon, BRC

Alanesoon, AUTOCLEAR, Bata, BRISTOL, Canon, CommPort, CP PLUS enhancing vision, CODE 3, UTILITY DIADORA, DELTAPLUS, Dräger, econosto, ECA Group

EPE, EVAC+CHAIR International, FirePro, Gigi Industries (Pvt.) Limited, Gulf Defense Security Systems, Hytera, INVICTUS, JIANN LIH, KAVALCO, Kimberly-Clark, Life Safety, LOXY, MICROSENS

MIDITEC, MICROGARD, MOBOTIX, NAFFCO, PILOMAT, reece, RS DYNAMICS, SARENA, sensurity, SFFECO, SIEMENS, SpotterRF, STREAMLIGHT, WHITE ROSE, Zamil Group

Want to exhibit?

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

Previous Supporters: ASIS International, وزارة الصحة Ministry of Health, UL, iosh

2015 Sponsors: Dräger, Gulf Defense Security Systems, 3M, GFSP

Official CPD Member: CPD MEMBER The CPD Certification Service

Organised by: BME GLOBAL, Dhahran expo

Official Production House: la Familia

Official Housing Agent: global TRAVEL PARTNERS

2016 Media Partners: HOMELAND SECURITY RESEARCH www.hsrc.biz, Global Security Mag, SECURITY MIDDLE EAST www.securitymiddleeastmagazine.com, The BIG RED GUIDE, Gulf Fire, SourceSecurity.com, CDM CYBER DEFENSE MAGAZINE

www.sss-arabia.com

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

The challenges of mobile technologies

By Milica Djekic

The mobile technologies can offer many advantages such as a phone call communication, text messaging, the Internet connection, smart applications management and much more. As they may provide you all these benefits, they can also be a great source of threats and risks to their users. For instance, the majority of cell phones could be tracked through their calls, SMS or GPS capabilities. These may open many possibilities to potential security concerns, so it's getting obvious that these emerging technologies could find their applications within the crime's or terrorist organizations.

The capabilities of mobile technologies

In this context, when we talk about mobile technologies, we would mention the capabilities that cell phones can offer to us as well as discuss some potential drawbacks correlated to this area. First, the main advantage of your cell phone is that you can make a call. The evidence that the phone call has been made are normally available through different sorts of listings.

Also, the fact is the majority of the international as well as case calls have been monitored and recorded. The reasons for these are mainly linked to the security's requirements.

Next, the modern cell phones may provide you with the well-known texting capabilities as well as many Internet connection options. Through the investigation process as well as the international security's operations, these cell phone's capabilities could be tracked. As it's obvious, this may be so useful to crime's and terrorist groups due to they may track your cell phone's activities so easily as well.

Finally, everyone got aware of possible cell phone's tracing option which is possible if your battery is inside your device. The tools that can support you in this are publicly available for free everywhere on the web. Hope it's getting clear how greatly these can threaten someone's business, property or even life.

The security's concerns in this emerging field

When we say that your cell phone is so suitable to its phone calls, SMS messaging, Internet communication or GPS locating, we would suggest that as it's convenient to its users – it can be so helpful to security's threats that are in possession of some of many cell phone's activities tracking applications.

If we have in mind that those phone's activities trackers are available almost everywhere and all the threat needs to know is to download such a tool and review some of many online tutorials or the other web resources in order to get a necessary skill, it's getting so obvious how these mobile technologies advantages could be used for dark purposes.

For instance, if someone gets the information about your cell phone's number coping with the SIM card's details, such a person can easily get an access to your phone's calls, text messages, GPS location or some Internet activities. If that person is a security's threat, you would find that you are in a serious trouble. The legal permission to do the phone's activities monitoring and recording got authorities only and every individual doing so on his own behalf is breaking the law.

Also, these sorts of security's concerns are usually an introduction to some more severe criminal or terrorist offences and their purpose is to gather enough information to an illegal group which would use them to make a plan about their future crime's actions.

Practically, mobile technologies may be used for different sorts of stalking activities as well as information gathering operations. Non-rarely, these activities leave the serious consequences.

Some practical examples and possible scenarios

We all are witnessing the scenarios by which some organized crime or terrorist group committed the horrible crime and behind everything was a carefully planned and prepared action relying on the pervious information collection through the cyber means. The easiest way to find someone is through his cell phone. Someone's phone number could be obtained through a well-coordinated hacker's attack.

Once you get those SIM card's details, you can track such a person's phone calls, text messages and GPS location or simply hack his cell phone if it is online. It's a serious security's concern if someone tracks you for a long period of time and gets familiar with your habits, businesses or plans.

Here, we would not make any recommendations which tools could be the most suitable for an illegal phone's activities tracking. It's obvious they can be so simply found through the web search. The only thing we would highlight here is that if you decide to do so, you would leave a trace within a cyberspace, so a good investigation would certainly find the evidence you left.

Could we get protected from these threats and how?

If we talk about the protection from these sorts of threats, it's clear there is no absolute protection in terms of possible prevention from a breach. The cryptography could be assumed as one of the effective methods, but as it's known – every algorithm can be broken sooner or later, depending on an invested time and effort.

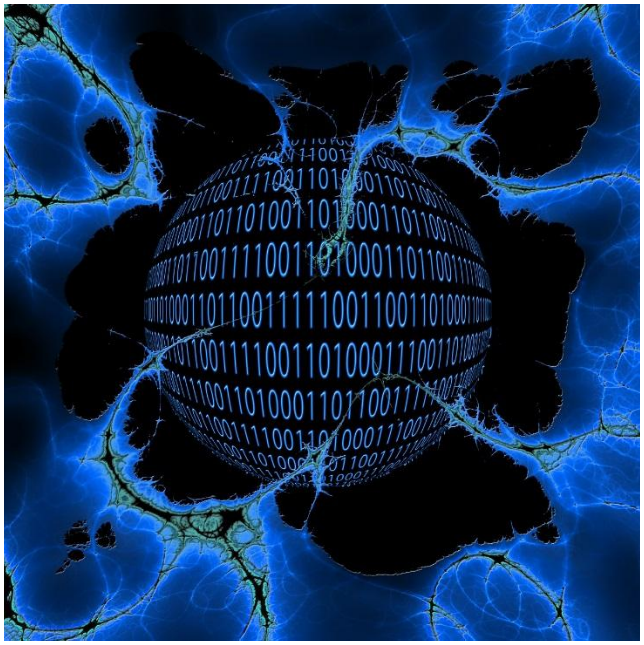
So, as many experts suggest we should try to accept that the breach has occurred and keep dealing with such a situation.

About the Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications. She writes for Australian and American security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

“Defense in Depth”

Jeff Michael, Senior Global Solutions Architect, Hexis Cyber Solutions



Cybersecurity has become a hot button issue across all industries.

Data breaches and cyberattacks are now the norm, and it has left companies scrambling to upgrade their cyber defenses and with that, organizations have begun to look into how to build their security “Defense in Depth.”

However, the term “Defense in Depth” has always concerned me. Organizations often think that defense in depth is equivalent to due diligence.

Due diligence is doing just enough to show that you are not liable.

However, what “Defense in Depth” means to most organizations is that they have deployed what they believe are the strongest tools at every layer of their network.

These layers are often the network layer, the desktop layer, and the application layer. However, it often seems like once these tools are deployed, it only highlights yet another area where more tools need to be placed.

What this means to the organizations is that they often spend a lot of time trying to find what they are missing, rather than focus on danger that may be around the corner.

What most organizations fail to realize is that the battle they are fighting is not a static battle, but a very dynamic battle. Imagine fighting an enemy that has unlimited resources.

These resources are dedicated to creating the best weapons, and training the best soldiers.

They are not focused on winning the battle, they are focused on destroying the enemy.

Destroying you may only take a few seconds because the techniques of the enemy are constantly evolving it makes the task of attempting to protect an organization almost impossible.

This would be like any modern army today engaging warfare against an army only equipped with World War 2 technology. No matter how great the defense is, the modern army will always win.

The best thing that organizations today can do is a combination of the following: strong policy enforcement, strong perimeter defenses, strong endpoint defenses, automated remediation, and very skilled malware specialists.

Advanced threat analytics should be important to any organization that takes its security posture seriously.

If an organization relies solely on legacy, signature-based detection, their defenses will be easily breached. It's important for teams to understand that the cyber defense and response capabilities of an organization must constantly evolve to match the evolving threat landscape.

Automatic remediation dramatically reduces the time that malware can exist on a network and also reduces the amount of time spent investigating the issue at hand.

And since these tools are automated and work at machine speed, they can deal with a high volume of threats without needing human intervention, easing the workload off of overburdened security teams, ultimately freeing them to act efficiently and effectively, before network damage is done.

About the Author

Jeff Michael joined Hexis in November 2014 as the Senior Global Solutions Architect.

He draws from over 15 years of experience in the cybersecurity industry, including positions at Trend Micro, FireEye, and NetWitness.

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

[Hexis Blog: http://www.hexiscyber.com/blog](http://www.hexiscyber.com/blog)

Twitter: @hexis_cyber

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

IT Security: Does Your Business Need a CISO?

Most people see the title *CISO (Chief Information Security Officer)* and automatically assume that it is a role handled solely by the IT department. While this is true, it's actually only part of their scope of work, mainly because the role extends to include an IT security consulting services function. To be effective, a CISO must have a broad perspective that allows them to perform their job of information security properly.

John Lyons, the chief executive of the International Cyber Security Protection Alliance, goes as far as to recommend that a CISO should be made an independent function altogether—one that is unencumbered by other agendas within the IT department.

He believes that the best ones for the job should be provided a budget to work with at their discretion to effectively keep both cyber attacks and costs at bay."

“If you have a CISO reporting through a CIO (Chief Information Officer) or if you put the cybersecurity budget in the technology budget, then the security spend gets lost among other priorities…it's right to segregate out the expenditure on security as a discrete part of the overall spend in the company,” Lyons added.

Does your business need a CISO? Here are the tell-tale signs that your organization can stand to benefit from one.

1. You need to cut costs.

Every business wants to reduce costs, but nobody wants to do so at the expense of having low-quality and inadequate security.

Having a CISO on board will greatly lower the risk of an attack, but often comes at a hefty price. After all, they bear a heavy burden of security for your business, and their services are becoming in-demand in today's wired and technology-driven commercial enterprises.

Most companies simply don't have the budget for a full-time CISO. So, one option is to hire someone to fill in the role on a part-time basis and share some of the responsibilities with an in-house CIO or IT team.

Another option is to get the services a virtual CISO, which is basically a third-party supplier that provides an IT consulting service.

2. There are no clear delineation of roles within the organization.

It is often the case that CIO's and board members will pay lip service, adding more financial and resource muscle to protecting their information, but in reality, not that much is allocated toward tighter security.

In Canada, for example, the average organization spends only about 6-10% on cybersecurity, according to a recent IDC survey. This is the typical scenario in most businesses, and there's often a conflict of interest in cases where a CISO's agenda is not in line the CIO's agenda to whom the former reports to.

Decision makers within a company might prioritize keeping costs down or introducing infrastructure changes, while a CISO might halt operations or slow things down in the name of cybersecurity.

When there's a CISO in charge of cyber security—whether in a part-time or full-time virtual capacity, these lines are clearly delineated, and their role in ensuring security is the only message they'll communicate to the decision makers. There will be no lumping of budgets to other IT needs, and the need for adequate online security will be given a voice within the organization.

3. Too much reliance on tools, not enough process training.

Businesses with bigger budgets will often invest in numerous anti-malware tools, but having all the bells and whistles in place is seldom enough.

Take the case of Target, a recent victim of an information breach that resulted in millions of dollars in liabilities. They were not remiss in installing cyber security tools that will detect malware - the invested $1.6 million on malware detection alone - and yet did not stop them from being viciously attacked online. The reason? Those in charge of looking after these warning chose to ignore them. The people who were supposed to put a plan into place when an indication of this magnitude should occur simply did not know what to do. There was no clear-cut process for them to follow.

Having a CISO accountable for these steps will ensure that the tools installed will be coupled by people who know how to use it correctly, and respond immediately to an imminent attack.

4. Little awareness or appreciation of what effective cyber security requires.

Most people think that all they need is to install an anti-virus, and they're all set to call it a day. That may have been true decades ago, but that's no longer the case today Attackers are becoming more sophisticated, and the tools they use are becoming harder to detect. A CISO whose primary responsibility is to discover any inconsistencies in their company's online landscape is required to ensure that your business is on top of things, and that there is minimal to no disruption in your business operations in the event of an attack.

They will also be in charge of providing adequate training and information dissemination programs, which make sure everyone in the company understands what they can do to keep their data and information intact.

5. You need to be compliant, but don't know where or how to start.

In response to increasing security risks, governments and other institutions have enforced standards and compliance requirements to ensure that security is prioritized in various businesses. In most cases, you need to be fully compliant before you can begin operations.

A virtual CISO would have the expertise to know the steps you need to take to receive adequate certification, and they'd be the go-to people you can consult for any updates within the industry. Cyber-security is a holistic pursuit that can't be relegated only to the IT team. It is a real threat that will have a far-reaching effect throughout your organization, and as such everyone must be involved; it needs to be a concerted effort where relevant departments actively contribute to the goal of better security.

You will need one person to be in charge of this concerted effort, and that person is a CISO (or in some cases, a virtual CISO). He or she will see to it that the goal of adequate security is met and that accountabilities are crystal clear—without getting lost in other equally pressing agendas prioritized by other departments.

About the Author

Vladimir de Ramos has been in the IT industry for more than 22 years with focus on IT Management, Infrastructure Design and IT Security. Outside the field, he is a professional business and life coach, a teacher and a change manager.

He is also a certified information security professional, a certified ethical hacker & forensics investigator and a certified information systems auditor.

Check out Vlad's IT community here: http://www.aim.ph/

Indonesia Infrastructure Week 2015

AIRPORTS & AVIATION INDONESIA 2015

KONSTRUKSI INDONESIA 2015

IIICE 2015 INDONESIA INTERNATIONAL INFRASTRUCTURE CONFERENCE AND EXHIBITION

CONNECT EXPO COMM INDONESIA 2015

4 POWERFUL EVENTS UNDER ONE ROOF

4-6 NOVEMBER 2015 | JAKARTA CONVENTION CENTER

YOUR DIRECT ROUTE INTO THE INDONESIAN INFRASTRUCTURE MARKETS. ATTENDED BY OVER 10,000 TRADE VISITORS

IIW - Indonesia Infrastructure Week will once again bring together four important events under one roof, linking government, public and private sector specialists from the Infrastructure, Airports & Aviation, Construction and ICT communities.

It's an unparalleled opportunity for those working across these sectors to come together to build and strengthen existing business relationships, create new ones and plan and discuss the projects that will drive Indonesia's future growth.

Register FREE today at www.INDONESIAINFRASTRUCTUREWEEK.COM

Early registrants will benefit from:

- FAST TRACK ENTRY
- access to the Global Meetings Programme
- chance to WIN AIR TICKETS

Hosted by

Ministry of Public Works and Housing Republic of Indonesia

Construction Services Development Board

Angkasa Pura | AIRPORTS

MTI

ANGKASA PURA II

mastel

DETIKNAS

Steering Committee

KADIN Indonesia Indonesian Chamber of Commerce and Industry

APPSI Association for Provincial Government of Indonesia

Supported by

BKPM Indonesia Investment Coordinating Board

Coordinating Ministry for Economic Affairs Republic of Indonesia

Bappenas Ministry of National Development Planning

Ministry of Transportation Republic of Indonesia

Coordinating Ministry for Politic, Legal and Security Republic of Indoneisa

Ministry of Communication and Information Technology Republic of Indonesia

IIW'15 Official Airline Partner

Batik air

IIW'15 Official ICT Partner

Telkom Indonesia

IIICE'15 Sponsors

Vermeer EQUIPPED TO DO MORE.

SMi

KI'15 Sponsor

JASAMARGA Indonesia Highway Corp.

CECI'15 Sponsor

accenture High performance. Delivered.

Q2 TECHNOLOGIES securing the unsecured

AAI'15 Sponsor

ARUP

Academic Advisor

Center for Sustainable Infrastructure Development

IIW'15 Official Media Partner

MNC GROUP

Media Partner

CDM CYBER DEFENSE MAGAZINE

Organized by

infrastructure asia

Tarsus Tarsus Group plc

Apple OS X Gatekeeper - When a Good App Goes Rogue

Apple's OS X Gatekeeper provides attackers with an easy way to deploy malicious software

by Kowsik Guruswamy, CTO, Menlo Security

Apple is known for delivering safe platforms that are protected from sophisticated attacks, but recently, an exploit was discovered in its OS X operating system that gives attackers an opportunity to install malicious code.

The exploit takes advantage of this flaw in OS X's "Gatekeeper" feature, which authenticates that the software being installed on an Apple Mac is secure enough to do so.

Ironically, Gatekeeper was designed to stop Trojan horse-style malware, but it only analyzes applications during installation, not any time after.

In order to exploit Gatekeeper, hackers simply needed to use a "trusted" Apple file and trick the OS X into deploying a malicious file that's stored in the same file folder as the trusted Apple file.

This is a classic case of bait-and-switch, where the app starts by offering something good to the user and then turns bad due to flaw exploitation.

We've seen this behavior in a number of other places including several productivity apps from the Chrome store, Google Play games that quickly gained popularity and began serving malware, and we've also seen Chrome extensions that blocked ads that were eventually purchased by a larger company to allow ads of their own.

According to Ars Technica, the crux of the problem is this: "The Gatekeeper's sole function is to check the digital certificate of a downloaded app before it's installed, to see if it's signed by an Apple-recognized developer or originated from the official Apple App Store.

It was never set up to prevent apps already trusted by OS X from running in unintended or malicious ways, as the proof-of-concept exploit the researcher developed does."

Once Web code or content of any kind reaches the endpoint, it's game over.

Further, the Gatekeeper bypass is significantly more severe than the recent Xcode Ghost because unlike Xcode Ghost where hackers trojanized the Xcode development toolchain and placed it on a server in China for "faster downloads," this Gatekeeper bypass vulnerability is an Apple-signed package downloaded from the Apple Store.

And users tend to trust this somewhat blindly, which is mistake all in itself.

Apple is still working on a patch to protect users from the vulnerability that was discovered by security researcher Patrick Wardle from Synack.

The broader implications of the vulnerability highlight the importance of not solely relying on static analysis, which is a moment-in-time snapshot check of good versus bad.

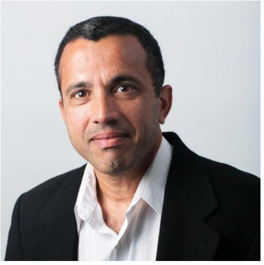
The security industry is still learning that using legacy technologies that determine good content from bad content do not stop malicious attacks from infecting users.

Even in the Web, we see sites like Forbes and Huffington Post - sites that are categorized as good - turn around and end up serving malware to unsuspecting users.

As much as it's against the grain, users would be better off limiting the number of apps they are running on their devices, especially from ones that are not trusted.

With the rise in malvertising, it’s also better to pay the 99 cents for an app than have it display ads from questionable sources.

About Kowsik Guruswamy



Kowsik Guruswamy is CTO of Menlo Security. Previously, he was co-founder and CTO at Mu Dynamics, which pioneered a new way to analyze networked products for security vulnerabilities. Prior to Mu, he was a distinguished engineer at Juniper Networks.

Kowsik joined Juniper via the NetScreen/OneSecure acquisition where he designed and implemented the industry's first IPS.

He has more than 15+ years of experience in diverse technologies like security, cloud, data visualization, and computer graphics.

Kowsik has 18 issued patents and holds an MSCS from University of Louisiana.

Kowsik can be reached online at (@K0ws1k) and at our company website https://www.menlosecurity.com/.

The Most Important Question to Ask Before Data Recovery

When a business or person needs a data recovery service provider, it's highly important to be sure the facility has the proper industry certifications. Otherwise, the data missing may be at a much higher risk of being unrecoverable or even permanently destroyed. First, let's take a look at why data recovery can be a dangerous feat.

The Dangers of Microscopic Particles in Data Recovery

As the platters in a hard disk drive (HDD) speed along at an average rate of 7,200 RPM, a cushion of air is created on which the actuator arm and read/write heads float a mere three nanometers above the fragile surface of the rotating disks. Known as "fly height"' this microscopic distance is essential to the functionality of the drive.

Extreme damage and permanent data loss can result if any particulate matter (even something as thin as a human fingerprint) gets between the surface of the rotating disk and the read/write heads. *Any* foreign object could be struck by one of the heads, causing damage to the mechanism and permanent destruction of data. Therefore, the data recovery company you choose with your data should have Certified ISO Class 5 Cleanroom, at least. Cleanrooms are often found within medical fields, like pharmacology and epidemiology. For perspective, in an average outdoor environment, one cubic foot of air could contain more than 35 million particles bigger than 0.5 microns in diameter (dust, dirt, ash, smoke, etc.). Indoor air is a bit cleaner, although there could still be roughly one million similar-sized particles in a cubic foot of atmosphere from an indoor location.

In an ISO Class 5 Cleanroom like the one at DriveSavers, less than 100 particles bigger than 0.5 microns are present per cubic foot of air, making it safe to open up and work on hard drives and other sensitive data storage devices without fear of contamination.

The Cleanrooms at data recovery companies allow engineers to open sealed drive mechanisms in accordance with all leading hardware and storage device manufacturers' specifications *without* voiding the original warranty. In a certified Cleanroom, drives and other sensitive equipment can be inspected and worked on without introducing any additional risks of contamination, damage or data loss.

Keeping the Cleanroom "clean"

Regular audits should be conducted to measure and certify the effectiveness of a Cleanroom installation while it's in use. Some data recovery companies with certified Cleanrooms had their audits performed while the rooms being tested were unoccupied and not in operation. Particle counts may differ substantially while a Cleanroom is actually in use and occupied with people.

Cleanroom engineers must wear special suits, in addition to protective head and footgear to guard against contamination. All accessories—including writing paper and pencils, cleaning tools and more—are designed specifically to reduce the release of any particulate matter into the atmosphere. How do you know if the audit was performed while the Cleanroom was in use or not?

Request the “Controlled Environment Testing Report” and look for “Occupancy State.” The status of the Occupancy State could be one of three: “as-built”, “at-rest” or “operational.” You want to see “operational.” Most Certified ISO Class 5 Cleanrooms allow engineers to work within the manufacturer recommended limits of cleanliness during the recovery process.

Glossary of Terms

Head spinning a bit? In order to understand the best place for your data recovery, we’ve included some terms to help get a clear picture. They are given in order as they appear in the article.

HDD: Hard disk drive

Read/Write Heads: The mechanisms that record and retrieve information on an HDD

Platters: Spinning disks in an HDD on which data is written and stored

Actuator Arm: The armature from which the read/write heads are suspended over the platters in an HDD

Fly Height: The distance between the platters and the read/write heads in an HDD—3 nanometers, or about 3/1,000,000,000th of an inch

Cleanroom: A customized laboratory environment in which the air is filtered continuously to reduce the amount of particulate matter present

Micron: A unit of measurement equal to 0.000039 inches

About the Author

As Director of Engineering, Mike Cobb manages the day-to-day operations of the Engineering Department including the physical and logical recoveries of rotational media, SSDs, smart devices and flash media. He also oversees the R&D efforts for past, present and future storage technologies. Mike makes sure that each of the departments and their engineers are certified and that they continue to gain knowledge in their field. Each DriveSavers engineer has been trained by Mike to ensure the successful and complete recovery of data is their top priority. Mike Cobb has a B.S. degree in Computer Science from the University of California, Riverside. Since joining DriveSavers in 1994, Mike has worked on all aspects of engineering as well as heading the Customer Service Department for several years. Prior to joining DriveSavers, Mike gained invaluable experience creating mirroring and compression products while working at Golden Triangle Software in the early 1990’s.

The Race to Resolution

Jeff Michael, Senior Global Solutions Architect, [Hexis Cyber Solutions](#).

When Indy car racing had its debut many years ago it looked nothing like it does today.

The average speed of the cars was 75mph, with today's cars going more than 200mph. As technology evolved, so did the car and the driver.

From 1911 to 1922 all cars had a riding mechanic onboard.

"A riding mechanic was a mechanic that rode along with a race car during races, and who was tasked with maintaining, monitoring, and repairing the car during the race.

The various duties included manually pumping oil and fuel, checking tire wear, observing gauges, and even massaging the driver's hands. They also communicated with the pits and spotted from inside the car.

If the car ran out of fuel, or otherwise broke down, the riding mechanic was usually responsible for running back to the pits to fetch fuel or the necessary spare parts." (Link)

Every task and every communication was handled manually. In today's Indy cars the Pit can automatically assess and monitor every variable of the car.

In addition, the Pit can be in constant communication with the driver.

The Pit crew can now take the information it receives from the car and correlate it with the information received from the driver to make the car and driver as competitive as possible.

Today's networks really aren't any different.

Most organizations today are still using technology that requires very manual tasks, and multiple people working numerous jobs to just maintain their existing security stance.

Just like the riding mechanic, it is often an overwhelming task with little or no success. Except, unlike the riding mechanic, the job of securing a network never ends.

Almost everything that happens in an enterprise passes through the network.

This has made business operations much more efficient, but has also left them vulnerable to cyberattacks.

A new study from Juniper Research suggests that this heavy reliance on business and consumer data will cause the cost of a data breach to balloon to a whopping 2.1 trillion dollars globally by 2019.

The growing prominence of mobile devices and the Internet of Things has given hackers new endpoints to exploit and they have major incentives to do so.

Cybercrimes like the theft of intellectual property, financial information or identity data, are becoming increasingly lucrative for hackers that want to sell their bounty on the black market.

In order to better utilize all assets that are designed to help organizations win the race of securing a network, continuous threat detection and automated response must be adopted.

With continuous threat detection and remediation, this automation removes the need for manual remediation and allows your users to focus on making your organization faster and more secure than ever.

These solutions allow your network to be like the modern day Indy cars: everything automated, with very little to no intervention required.

About the Author

Jeff Michael joined Hexis in November 2014 as the Senior Global Solutions Architect.

He draws from over 15 years of experience in the cybersecurity industry, including positions at Trend Micro, FireEye, and NetWitness.

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

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

Twitter: @hexis_cyber

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

GLOBAL CYBER SECURITY LEADERS 2015

EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

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

IMPROVING THE STATE OF CYBER SECURITY IN THE DIGITAL AGE

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

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

Presentations include:

Hoang Bao

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

Alexander Oesterle

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

Jakub Boratynski

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

Kim B. Larsen

CSO, **Huawei Technologies, Denmark**

Dr. Bernd Eßer

Head of Cyber Defense & CERT, **Deutsche Telekom AG, Germany**

Uday Deshpande

CISO, **Tata Motors, India**

Arieh Shalem

CISO, **Orange Telecommunication, Israel**

Gianluca Varisco

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

Official Part of

Global Leaders Summit Series
EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

Mediapartner

CDM
CYBER DEFENSE MAGAZINE

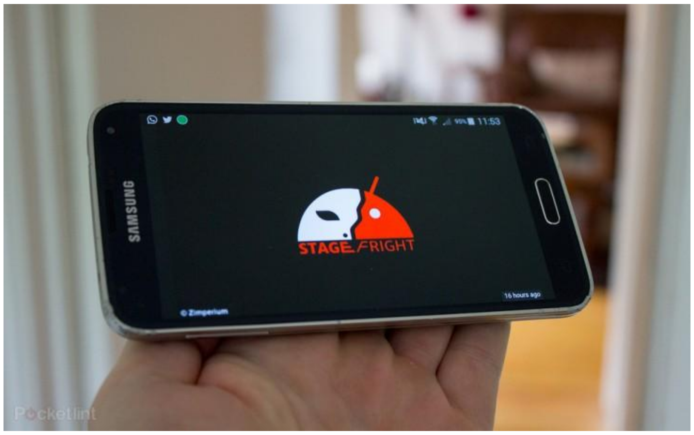
Hosted by

25 YEARS EXPERIENCE MANAGEMENTCIRCLE®

www.cybersecurity-leaders.com

Why every Android user should take the Stagefright leak very seriously

A vulnerability in Android called Stagefright was exposed at the 2015 Black Hat conference in early August. You may have heard of it, if only because the media frenzy that followed claimed that hundreds of millions of phones could be hacked with a single text – but is any of that true? If that were the case, surely Google, the developer of the popular operating system, would have fixed it by now…right?



(image: pocket-lint.com)

What is Stagefright and why should you care?

You may have grown accustomed to all of the vulnerabilities, bug and alerts out there in technology land. You're calm because you know that ultimately there will be a patch to fix it, right?

Unfortunately, it's not so simple with the Stagefright leak. Think of a doomsday film where a deadly asteroid is about to strike Earth, and there's no way for scientists to divert it with their fancy technology. That's basically what's going on – the Stagefright bug, due to the nature of the Android world, isn't likely to be addressed any time soon. If things don't change, it's only a matter of time before an exploit strikes and brings chaos to an unthinkable number of devices.

So, yes, it is possible that you could receive a strange video text, not even open it, and some cyber criminal halfway around the world could start spying on you through your video camera. But that's only one possibility.

If a hacker gets into your device through the Stagefright vulnerability, he could gain access to your address book, apps, message history, personal emails, and all the information tied to your Google account. This means that every bit of information tied to your Google account – from Gmail to Google Drive – is up for grabs: financial information, browsing history, personal messages and classified work documents…

It's imperative you understand that your phone isn't the only thing at risk. Your whole digital life is at risk.

How does Android work, exactly?

To understand the Stagefright vulnerability properly, it's important to look at the Android architecture. Android is very modular operating system, so things run in separate processes. This is in part thanks to the Dalvik virtual machine, which is the component in most Android phones (it has been replaced entirely by Android runtime in Android 5.0) that allows each app to run separately and independent of the Linux kernel. This keeps apps from detrimentally interfering with each other or with the operating system.

This means program processes rely on IPC or inter-process communications to work together. This is known as application sandboxing (or application containerization), and one of the alleged advantages of this is that keeping applications isolated improves overall security.

Stagefright is what processes media in Android's MediaServer, written primarily in C++. It handles all video and audio files, and provides playback facilities. It also extracts metadata for the Gallery (like thumbnails or dimensions of a video).

How Stagefright reaches you

So it might be fair to assume that since the programs on your phone are sandboxed, most aspects of the system are safe from a single vulnerability. But while the compartmentalized nature of Android is supposed to keep programs from interfering, MediaServer is a very privileged service that has access to audio, bluetooth, camera, internet, and more. What's worse, many phone manufacturers have given the Stagefright component system permissions on their devices, which is only a step below root access.

In layman's terms: a hacker could gain access to your entire device.

An attacker only needs your phone number to conduct a successful hack. He or she could remotely execute code through a video sent via MMS. It would require no action on your part, as Android phones are set to preload videos. The attacker can even delete the message after sending it, leaving you with little more than a mysterious notification.

If that doesn't sound horrifying enough, that isn't the worst of it. The reality is, that's just one way that the vulnerability can be exploited. It's up to the hackers of the world to discover the rest.

Who figured this out?

Joshua J. Drake, an Android security expert, is the man behind the research. He is the Senior Director of Platform Research at Zimperium Enterprise Mobile Security, and the Author of "Android Hacker's Handbook". He's also the founder of the #droidsec research group, an Android-focused research community.

With the support of Zimperium and Optiv, Drake conducted this security research, using his “droid army” – a collection of 51 Android devices. You can learn more about how he conducted his research in his presentation at the Black Hat conference in Las Vegas.

A fragmented Android world

Android is one of the world’s most popular operating systems and it has a unique story. The rate of development is incredibly fast, but that development doesn’t come without a price. Since original equipment manufacturers and carriers are able to adapt the operating system due to its open source nature, this leads to a number of iterations that have unique update and patching needs – over 24,000 models currently exist in the Android ecosystem.

The biggest problem with this vulnerability, as *Ars Technica* writer Ron Amadeo points out, is that original equipment manufacturers have been able to adapt the Android code to work with their devices. This creates a dilemma where an unthinkable amount of patches would have to be made in order to successfully protect the majority of Android phones out there, and no single company, team, or entity is responsible for getting this issue under control. Because updates will focus on newer phones, and many patches will be dependent upon a myriad of manufacturers and carriers to distribute them, it is possible that millions to hundreds of millions of devices will remain vulnerable indefinitely.

What’s being done?

Google, as well as number of manufacturers and carriers have responded with patches for the following devices.

Zimperium has also launched its ZHA Alliance to address the issue of communication between relevant manufacturers and carriers on the issue. As Zimperium so aptly stated, “According to our understanding of the Android ecosystem, security issues reported to Google are only shared with active partners”.

Zimperium has also released an app known as the Stagefright Detection app, which can help you identify if your phone is actually affected by the vulnerability.

So what’s the problem?

You might think that since the patches are rolling out, there shouldn’t be any further problems. Surely the patches will trickle down to older phones, and Zimperium will help facilitate that communication between Google, carriers, and manufacturers

Even if that is the case and the majority of phones get patched up, there may be an issue with the effectiveness of Google’s first patch. Security researcher Jordan Gruskovnjak at Exodus Intelligence has reported that the initial patch released by Google was inadequate. The Exodus team was able to craft an MP4 that could bypass the patch. They even claim that Zimperium’s Stagefright Detection app will green-light your patched phone, even though it’s still vulnerable.

Google has responded to the situation, asserting in a statement to *The Verge*, “We’ve already sent the fix to our partners to protect users, and Nexus 4/5/6/7/9/10 and Nexus Player will get the OTA update in the September monthly security update”.

If that wasn’t bad enough, Rob Miller from MWR Labs has found another vulnerability that can bypass the sandbox mechanism. Originally reported back in March, it seems that Google has yet to release a relevant patch. Researchers at Trend Micro have claimed to have also found a vulnerability, this time in Android MediaServer, which they reported to Google back in June (Google published a fix in early August).

The reality is, even if Google’s next patch is effective it doesn’t address the full story. The Stagefright media circus simply revealed a can of worms that opened long ago – Android has some major security flaws, and the broken chain of distributors and manufacturers makes it nearly impossible to rectify.

What you can do

If you have an Android phone with version 2.2 or higher, it may seem that there isn’t much left in your control. But we encourage you to do all you can to take security into your own hands.

While it’s true that there are limits to your autonomy in the face of all of the vulnerabilities your phone could be riddled with, there are several steps you can take to make your experience on Android safer. Even if you don’t have an Android phone, you can use these tips and apply them to your own smartphone experience.

Change your settings

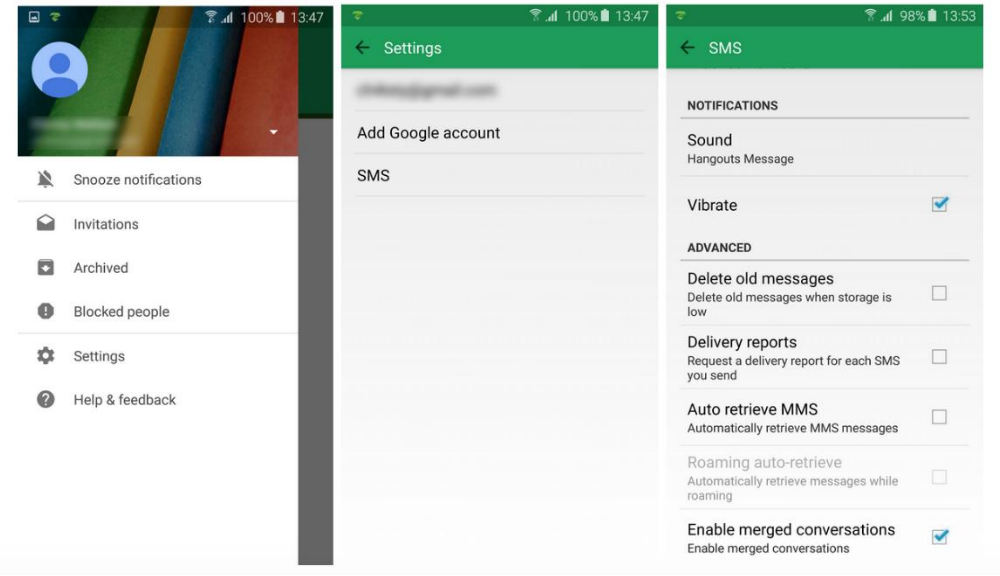
It’s important to acknowledge that while Zimperium illustrated an exploit through MMS and that’s what the media has held onto, this is just an example of how the vulnerability can be exploited, so disabling auto-retrieval will not necessarily protect you from all possible hacks. Joshua J. Drake himself said at the Black Hat conference that the Stagefright bug is exposed via multiple attack vectors.

With that being said, the MMS attack has been receiving a lot of attention, and it’s possible that cyber criminals are getting ideas. So it’s best to deactivate auto-retrieval as it preloads videos and messages for you. Here is how to disable the auto-retrieval feature on the most common messaging applications:

Google Hangout

Open the app and select Settings by tapping the three horizontal lines in the top left corner.

Click the Settings wheel and then select SMS. Uncheck Auto-retrieve MMS.



100% 13:47

[redacted]

Snooze notifications

Invitations

Archived

Blocked people

Settings

Help & feedback

100% 13:47

Settings

[redacted]

Add Google account

SMS

98% 13:53

SMS

NOTIFICATIONS

Sound
Hangouts Message

Vibrate ☑

ADVANCED

Delete old messages
Delete old messages when storage is low □

Delivery reports
Request a delivery report for each SMS you send □

Auto retrieve MMS
Automatically retrieve MMS messages □

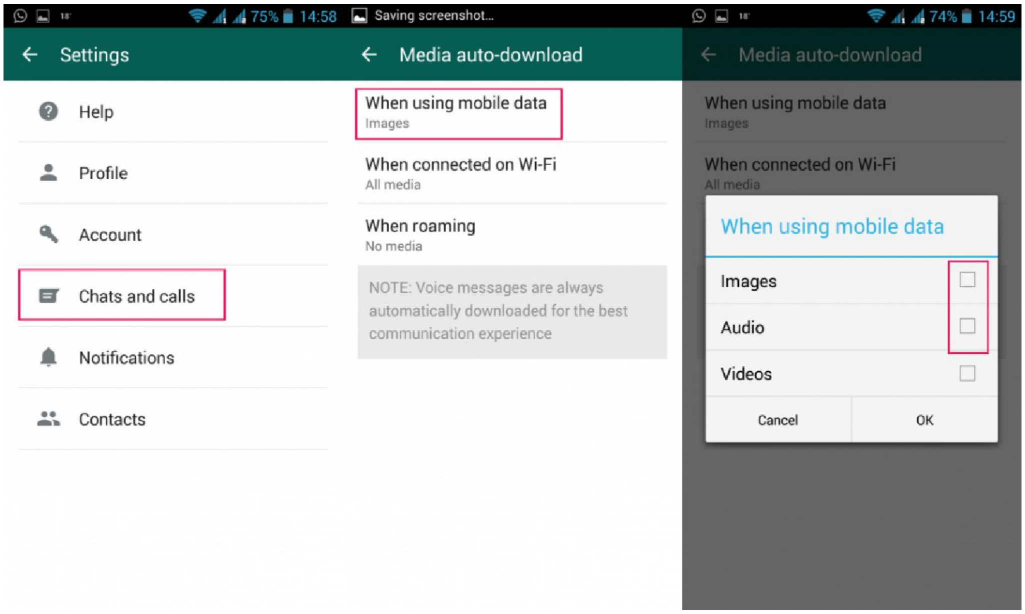
Roaming auto-retrieve
Automatically retrieve messages while roaming □

Enable merged conversations
Enable merged conversations ☑

Source: Zimperium

WhatsApp

Select Settings by clicking the three dots icon, and then select Chat Settings. Tap Media auto-download and go to the When connected on Wi-Fi. Deselect videos, and then do the same under the When using mobile data option.



75% 14:58

Settings

Help

Profile

Account

Chats and calls

Notifications

Contacts

Saving screenshot...

Media auto-download

When using mobile data
Images

When connected on Wi-Fi
All media

When roaming
No media

NOTE: Voice messages are always automatically downloaded for the best communication experience

74% 14:59

Media auto-download

When using mobile data

Images □

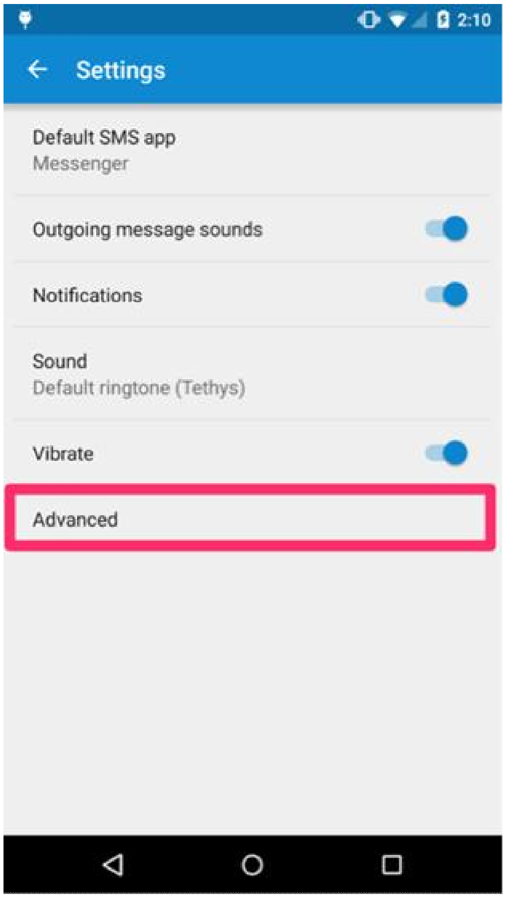
Audio □

Videos □

Cancel OK

Google Messenger

Touch the three vertical dot icon in the upper right corner. Select Settings and then Advanced. Then deselect Auto-retrieve.



2:10

Settings

Default SMS app
Messenger

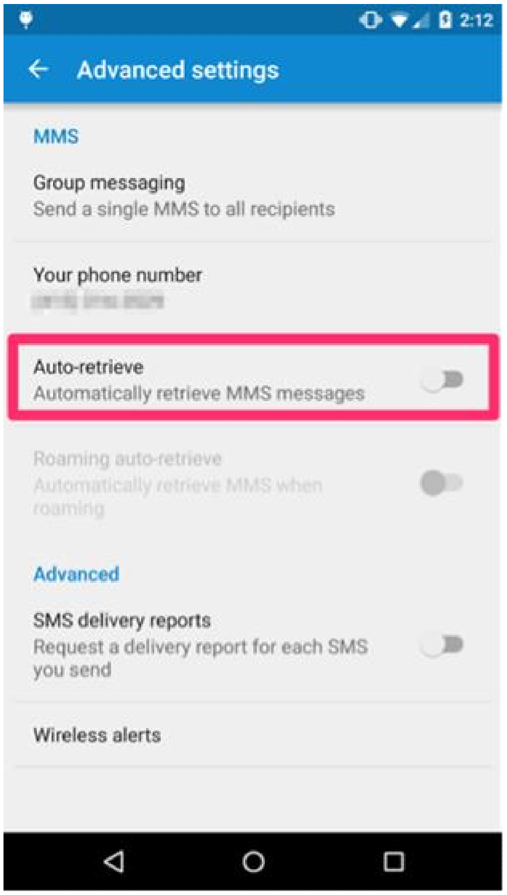
Outgoing message sounds ●

Notifications ●

Sound
Default ringtone (Tethys)

Vibrate ●

Advanced



2:12

Advanced settings

MMS

Group messaging
Send a single MMS to all recipients

Your phone number
[redacted]

Auto-retrieve
Automatically retrieve MMS messages ○

Roaming auto-retrieve
Automatically retrieve MMS when roaming ○

Advanced

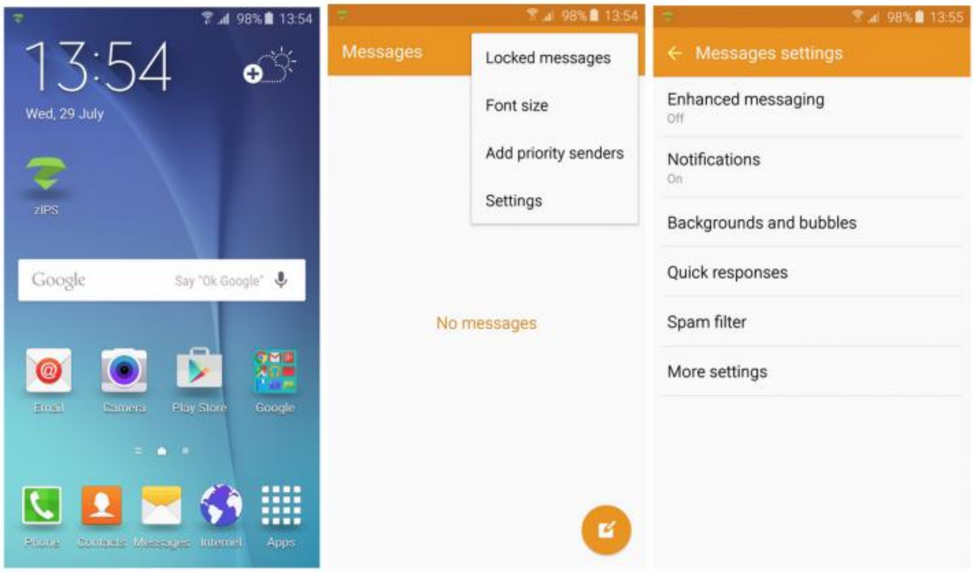
SMS delivery reports
Request a delivery report for each SMS you send ○

Wireless alerts

Messages

Navigate to More and select Settings, then More settings.

Click Multimedia messages and then slide the Auto retrieve toggle to the left.



Messages settings

Enhanced messaging
Off

Notifications
On

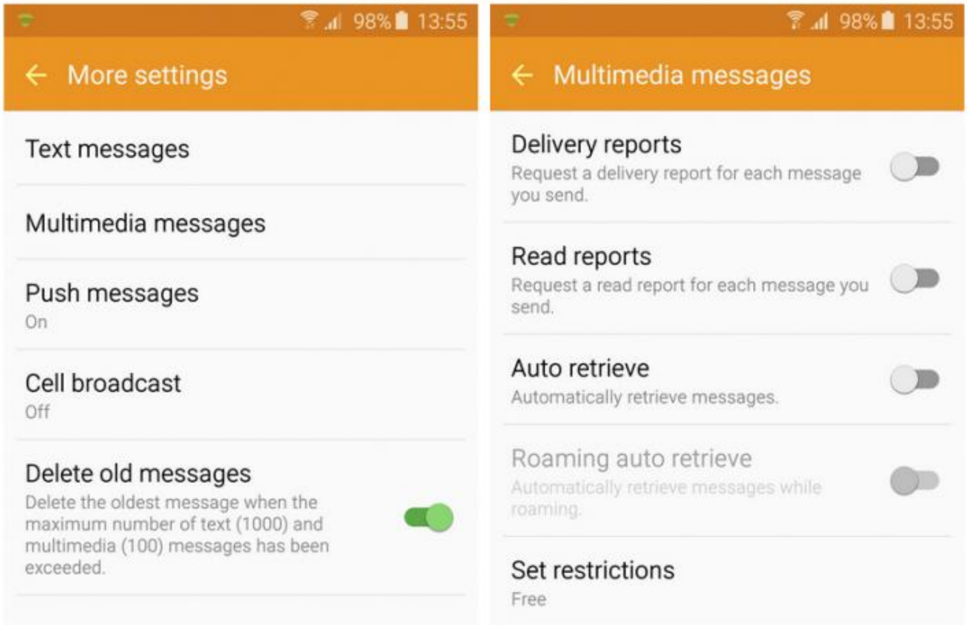
Backgrounds and bubbles

Quick responses

Spam filter

More settings

Source: Zimperium



More settings

Text messages

Multimedia messages

Push messages
On

Cell broadcast
Off

Delete old messages
Delete the oldest message when the maximum number of text (1000) and multimedia (100) messages has been exceeded.

Multimedia messages

Delivery reports
Request a delivery report for each message you send.

Read reports
Request a read report for each message you send.

Auto retrieve
Automatically retrieve messages.

Roaming auto retrieve
Automatically retrieve messages while roaming.

Set restrictions
Free

Source: Zimperium

Even after deactivating auto-retrieval, be wary of manually loading an MMS from an unknown source, and if you want to be extra safe, don't load one from friends or family either. They can unknowingly put you at risk if their phone is compromised.

Your consumer choices

While most normal people don't have the resources to buy the latest and greatest model of every device, it's important to consider the likelihood that future devices will be more secure than current models. Additionally, important security patches and updates generally won't be released to devices that can't support newer versions of Android.

Remember to educate yourself on the operating systems and programs you use, and vigilantly update to newer versions if possible. For example, the Mozilla Firefox browser was also affected by the Stagefright vulnerability, but the issue has been rectified since version 38.

Make your voice heard

Just because the mainstream media has dropped the issue as of late doesn't mean the Stagefright bug doesn't affect millions of people around the globe. Voice your own concerns and demand that your carrier keep you updated on the issue. Make noise on your social media channels and tag Google, your carrier, and your manufacturer in your posts. Forward articles related to the Stagefright issue to your Android-using loved ones.

Switch your operating system

This is an option for more experienced users and not a recommendation for most people. Still, it is an option and should be discussed with more regularity. If your inclined to try this option, consider using firmware with a regularly updated ROM, such as CyanogenMod. You will need to root your phone, and if you do this you will most likely lose your warranty with your manufacturer. Also be aware that this move will not make you 100% clear of the Stagefright vulnerability or other bugs. The advantage is that you have an Android device, but the hassle of waiting on manufacturers and carriers to adapt patches is removed, and you can receive updates more immediately.

As the months go by, we can only hope that there is a real solution to this issue. Remember to stay informed about security updates, subscribe to newsletters, and follow security blogs. Talk to your friends and family, and assert your rights to privacy and safety as a consumer. While developments in technology move at an impressive rate, there's no point in having all of these fancy devices if we're moving towards a digital Armageddon. Remember, safety is just as important as progress.

Have a great, exploit-free day!

About the Author

Christian is the founder and a CEO of Emsisoft, a New Zealand anti-malware company. For CDM, his aim is to educate our readers with essential security knowledge, especially in understanding and stopping new and innovative malware.

Continuous Scanning

Francisco Amato, CEO, Infobyte LLC

Introduction:

Doing a security audit for your infrastructure, web site or services whether it be annually or every six months is a great first step to better securing your systems, but in many cases it is not enough.

Adding to that, if the audit only involves one tool, our attack surface unfortunately is pretty small.

The idea of this post is to tell everyone about how to use the Faraday platform to be able to do continuous scannings using almost all the auditing tools on the market.

The goal will be to do a scan every week or by events after a set of targets with different tools and obtain all the results on your Faraday platform. This should allow you to detect and mitigate new issues in your infrastructure.

While it is always necessary to conduct regular manual security audits (at least for the time being the software is not better than people). By doing continuous scannings it can help a company pick off a lot of the low hanging fruit and let them concentrate on trickier stuff.

Preparation:

We are going to use the following tools:

- w3af
- nmap
- nikto
- burp
- zap
- nessus
- openvas

Using a set of scripts together with different API we can obtain from a list of IPs/ Websites the corresponding reports.

Each report must be copied to $HOME/.faraday/report/[workspace_name]

Faraday than will convert all the reports into valuable information to be interpreted by the user.

Script:

The following script will centralize all the actions we mentioned before.

./cscan.py: #execute each script inside ./scripts/network/ and ./scripts/web/

./scripts/web #directory for web tools

```
./scripts/network #directory for network tools

./output #temporary directory where the reports are generated

./websites.txt #Website list

./ips.txt #IPs/Networks list

./plugin #plugin or library necessary for ./scripts/

./config.py #global configuration
```

The following is the nmap script

```
./scripts/network/nmap

NAME="nmap_$(date +%s).xml"
${CS_NMAP:=nmap} -iL $1 -oX $2$NAME
```

It very simply takes two parameters, the first is the target and the second the output directory for the report, it can be programmed in any languages, the following tools are available:

```
./scripts/web/burp.sh

./scripts/web/zap.sh

./scripts/web/nikto.sh

./scripts/web/w3af.sh

./scripts/network

./scripts/network/nmap.sh

./scripts/network/openvas.sh

./scripts/network/nessus.sh
```

Before starting to use it, review ./config.py as it contains specific configurations that can change your system, some include the path of the tools, openvas/nessus credentials, etc.

Schedule:

The last step is configure how regularly you are going to run the tool.

A simple example would be using cron each day at midnight executing the tool and moving the reports to the workspace "workspace_name"

# crontab -l

*0 0 * * * bash /root/dev/cscan/cscan.py ; mv /root/dev/cscan/output/* /root/.faraday/report/workspace_name/*

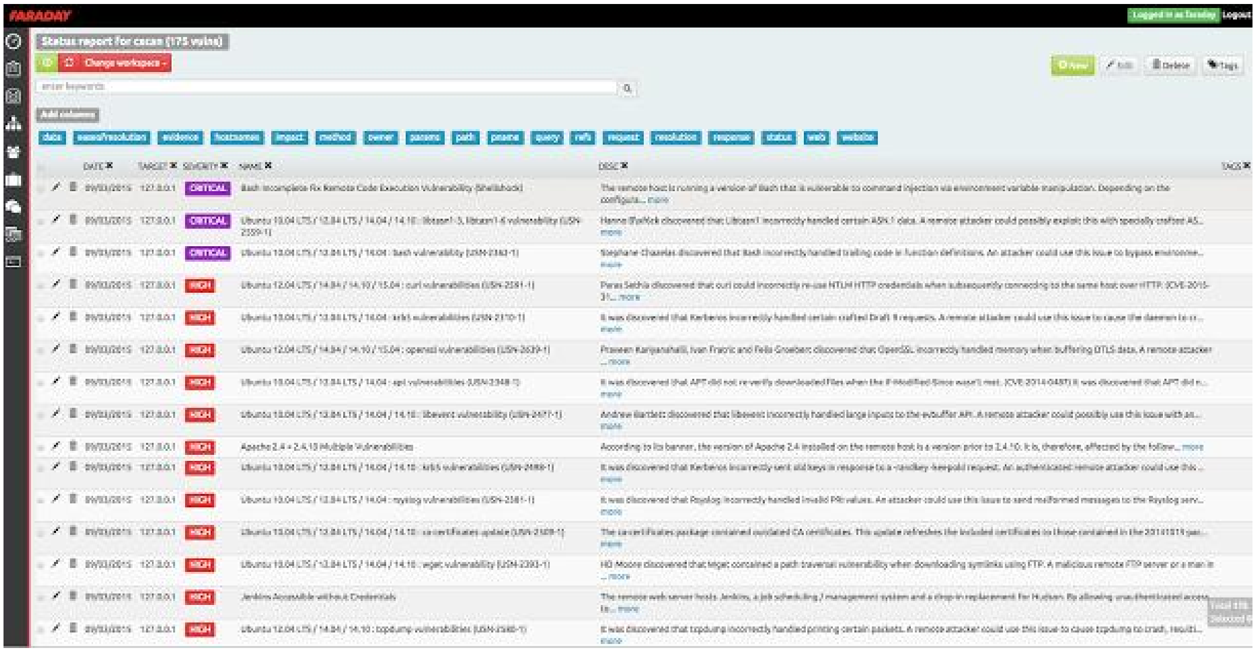
Another option is to configure the scripts with Jenkins and we would be able to set up different configurations with events do the scanning starts.

An example would be each time a new merge / release is done there it will be a scan of the web site or specific IP,

Faraday Web UI:

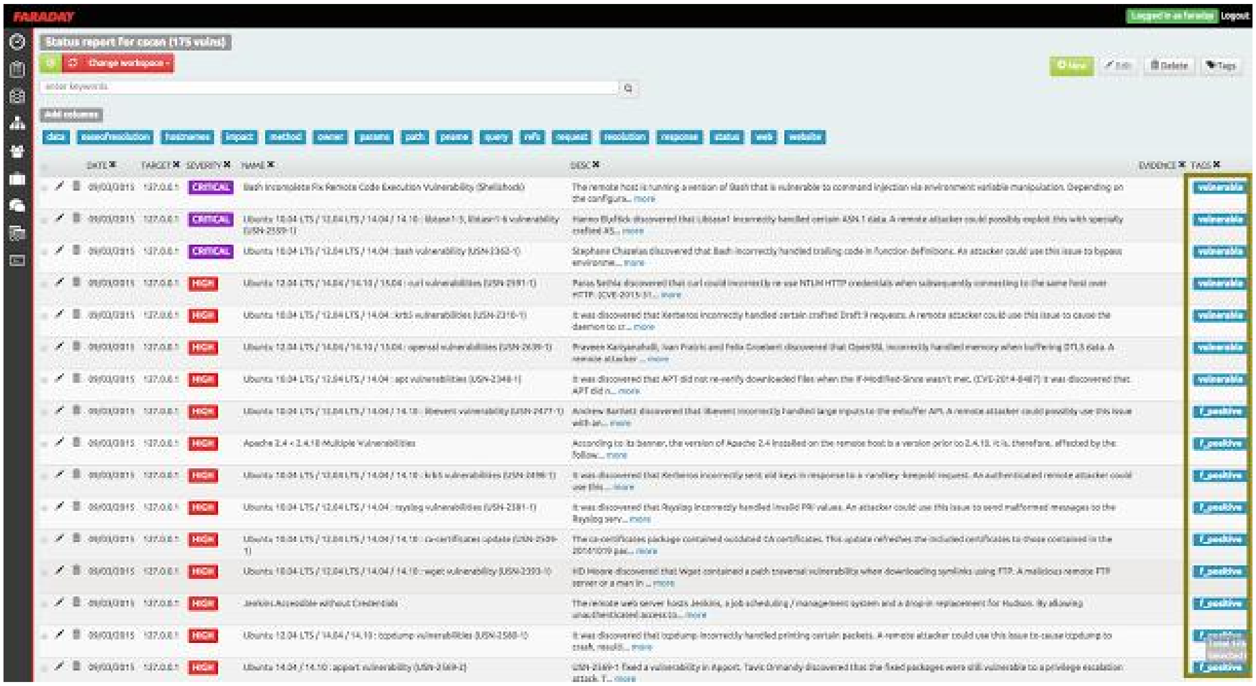
Each time a report is incorporated this will include only the new information. Using tags we can categorize the vulnerabilities where it is necessary to focus our attention.

1) In the image below we can see our first import from Nessus.



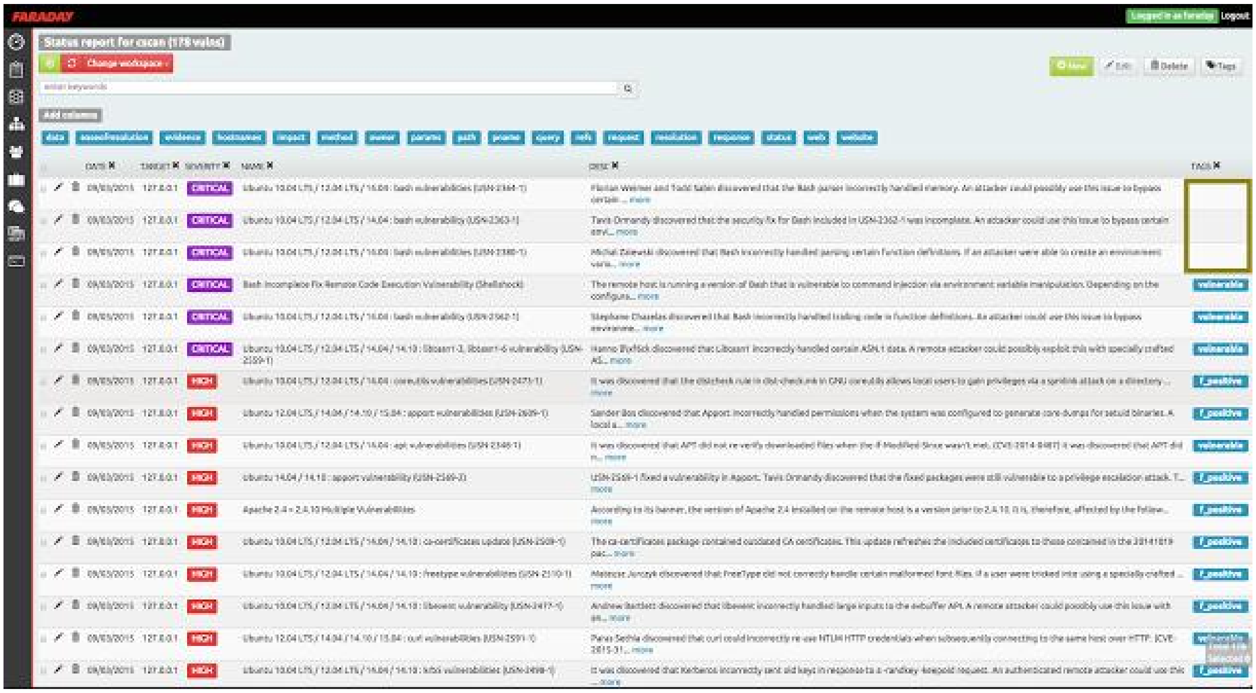
DATE	TARGET	SEVERITY	NAME	DESC	TAGS
09/03/2015	127.0.0.1	CRITICAL	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configura... more	
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libtasn1-3, libtasn1-6 vulnerability (USN-2559-1)	Hanno Böck discovered that Libtasn1 incorrectly handled certain ASN.1 data. A remote attacker could possibly exploit this with specially crafted AS... more	
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerability (USN-2362-1)	Stephane Chazelas discovered that Bash incorrectly handled trailing code in function definitions. An attacker could use this issue to bypass environme... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : curl vulnerabilities (USN-2591-1)	Paras Sethia discovered that curl could incorrectly re-use NTLM HTTP credentials when subsequently connecting to the same host over HTTP. (CVE-2015-31... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : krb5 vulnerabilities (USN-2310-1)	It was discovered that Kerberos incorrectly handled certain crafted Draft 9 requests. A remote attacker could use this issue to cause the daemon to c... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : openssl vulnerabilities (USN-2639-1)	Praveen Kariyanahalli, Ivan Fratric and Felix Groebert discovered that OpenSSL incorrectly handled memory when buffering DTLS data. A remote attacker ... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : apt vulnerabilities (USN-2348-1)	It was discovered that APT did not re-verify downloaded files when the If-Modified-Since wasn't met. (CVE-2014-0487) It was discovered that APT did n... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libevent vulnerability (USN-2477-1)	Andrew Bartlett discovered that libevent incorrectly handled large inputs to the evbuffer API. A remote attacker could possibly use this issue with an... more	
09/03/2015	127.0.0.1	HIGH	Apache 2.4 < 2.4.10 Multiple Vulnerabilities	According to its banner, the version of Apache 2.4 installed on the remote host is a version prior to 2.4.10. It is, therefore, affected by the follow... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : krb5 vulnerabilities (USN-2498-1)	It was discovered that Kerberos incorrectly sent old keys in response to a -randkey -keepold request. An authenticated remote attacker could use this... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : rsyslog vulnerabilities (USN-2381-1)	It was discovered that Rsyslog incorrectly handled invalid PRI values. An attacker could use this issue to send malformed messages to the Rsyslog serv... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : ca-certificates update (USN-2509-1)	The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 20141019 pac... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : wget vulnerability (USN-2393-1)	HD Moore discovered that Wget contained a path traversal vulnerability when downloading symlinks using FTP. A malicious remote FTP server or a man in ... more	
09/03/2015	127.0.0.1	HIGH	Jenkins Accessible without Credentials	The remote web server hosts Jenkins, a job scheduling / management system and a drop-in replacement for Hudson. By allowing unauthenticated access to... more	
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 : tcpdump vulnerabilities (USN-2580-1)	It was discovered that tcpdump incorrectly handled printing certain packets. A remote attacker could use this issue to cause tcpdump to crash, resulti... more	

2) In the second image we tagged the vulnerabilities, as a real vulnerability or a false positive.



DATE	TARGET	SEVERITY	NAME	DESC	EVIDENCE	TAGS
09/03/2015	127.0.0.1	CRITICAL	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configura... more		vulnerable
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libtasn1-3, libtasn1-6 vulnerability (USN-2559-1)	Hanno Böck discovered that Libtasn1 incorrectly handled certain ASN.1 data. A remote attacker could possibly exploit this with specially crafted AS... more		vulnerable
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerability (USN-2362-1)	Stephane Chazelas discovered that Bash incorrectly handled trailing code in function definitions. An attacker could use this issue to bypass environme... more		vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : curl vulnerabilities (USN-2591-1)	Paras Sethia discovered that curl could incorrectly re-use NTLM HTTP credentials when subsequently connecting to the same host over HTTP. (CVE-2015-31... more		vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : krb5 vulnerabilities (USN-2310-1)	It was discovered that Kerberos incorrectly handled certain crafted Draft 9 requests. A remote attacker could use this issue to cause the daemon to cr... more		vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : openssl vulnerabilities (USN-2639-1)	Praveen Kariyanahalli, Ivan Fratric and Felix Groebert discovered that OpenSSL incorrectly handled memory when buffering DTLS data. A remote attacker ... more		vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : apt vulnerabilities (USN-2348-1)	It was discovered that APT did not re-verify downloaded files when the If-Modified-Since wasn't met. (CVE-2014-0487) It was discovered that APT did n... more		vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libevent vulnerability (USN-2477-1)	Andrew Bartlett discovered that libevent incorrectly handled large inputs to the evbuffer API. A remote attacker could possibly use this issue with an... more		f_positive
09/03/2015	127.0.0.1	HIGH	Apache 2.4 < 2.4.10 Multiple Vulnerabilities	According to its banner, the version of Apache 2.4 installed on the remote host is a version prior to 2.4.10. It is, therefore, affected by the follow... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : krb5 vulnerabilities (USN-2498-1)	It was discovered that Kerberos incorrectly sent old keys in response to a -randkey -keepold request. An authenticated remote attacker could use this... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : rsyslog vulnerabilities (USN-2381-1)	It was discovered that Rsyslog incorrectly handled invalid PRI values. An attacker could use this issue to send malformed messages to the Rsyslog serv... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : ca-certificates update (USN-2509-1)	The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 20141019 pac... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : wget vulnerability (USN-2393-1)	HD Moore discovered that Wget contained a path traversal vulnerability when downloading symlinks using FTP. A malicious remote FTP server or a man in ... more		f_positive
09/03/2015	127.0.0.1	HIGH	Jenkins Accessible without Credentials	The remote web server hosts Jenkins, a job scheduling / management system and a drop-in replacement for Hudson. By allowing unauthenticated access to... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 : tcpdump vulnerabilities (USN-2580-1)	It was discovered that tcpdump incorrectly handled printing certain packets. A remote attacker could use this issue to cause tcpdump to crash, resulti... more		f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 14.04 / 14.10 : apport vulnerability (USN-2569-2)	USN-2569-1 fixed a vulnerability in Apport. Tavis Ormandy discovered that the fixed packages were still vulnerable to a privilege escalation attack. T... more		f_positive

3) Finally in the last image we loaded a second Nessus report and here we can observe the new vulnerabilities.



DATE	TARGET	SEVERITY	NAME	DESC	TAGS
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerabilities (USN-2364-1)	Florian Weimer and Todd Sabin discovered that the Bash parser incorrectly handled memory. An attacker could possibly use this issue to bypass certain ... more	
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerability (USN-2363-1)	Tavis Ormandy discovered that the security fix for Bash included in USN-2362-1 was incomplete. An attacker could use this issue to bypass certain env... more	
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerabilities (USN-2380-1)	Michal Zalewski discovered that Bash incorrectly handled parsing certain function definitions. If an attacker were able to create an environment varia... more	
09/03/2015	127.0.0.1	CRITICAL	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configura... more	vulnerable
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : bash vulnerability (USN-2362-1)	Stephane Chazelas discovered that Bash incorrectly handled trailing code in function definitions. An attacker could use this issue to bypass environme... more	vulnerable
09/03/2015	127.0.0.1	CRITICAL	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libtasn1-3, libtasn1-6 vulnerability (USN-2559-1)	Hanno Böck discovered that Libtasn1 incorrectly handled certain ASN.1 data. A remote attacker could possibly exploit this with specially crafted AS... more	vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : coreutils vulnerabilities (USN-2473-1)	It was discovered that the distcheck rule in dist-check.mk in GNU coreutils allows local users to gain privileges via a symlink attack on a directory ... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : apport vulnerabilities (USN-2609-1)	Sander Bos discovered that Apport incorrectly handled permissions when the system was configured to generate core dumps for setuid binaries. A local a... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 : apt vulnerabilities (USN-2348-1)	It was discovered that APT did not re-verify downloaded files when the If-Modified-Since wasn't met. (CVE-2014-0487) It was discovered that APT did n... more	vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 14.04 / 14.10 : apport vulnerability (USN-2569-2)	USN-2569-1 fixed a vulnerability in Apport. Tavis Ormandy discovered that the fixed packages were still vulnerable to a privilege escalation attack. T... more	f_positive
09/03/2015	127.0.0.1	HIGH	Apache 2.4 < 2.4.10 Multiple Vulnerabilities	According to its banner, the version of Apache 2.4 installed on the remote host is a version prior to 2.4.10. It is, therefore, affected by the follow... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : ca-certificates update (USN-2509-1)	The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 20141019 pac... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : freetype vulnerabilities (USN-2510-1)	Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted ... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : libevent vulnerability (USN-2477-1)	Andrew Bartlett discovered that libevent incorrectly handled large inputs to the evbuffer API. A remote attacker could possibly use this issue with an... more	f_positive
09/03/2015	127.0.0.1	HIGH	Ubuntu 12.04 LTS / 14.04 / 14.10 / 15.04 : curl vulnerabilities (USN-2591-1)	Paras Sethia discovered that curl could incorrectly re-use NTLM HTTP credentials when subsequently connecting to the same host over HTTP. (CVE-2015-31... more	vulnerable
09/03/2015	127.0.0.1	HIGH	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : krb5 vulnerabilities (USN-2498-1)	It was discovered that Kerberos incorrectly sent old keys in response to a -randkey -keepold request. An authenticated remote attacker could use this ... more	f_positive

This continuous procedure lets a company have an expanded vision overtime of their infrastructure.

Tool:

You can find the code on Github:

http://github.com/infobyte/cscan

In the next iteration of Faraday we are going to be distributing it within the tool sets in the directory*$FARADAY_DIR/scripts/cscan/*

Install:

*For burp it is necessary include the plugin plugin/carbonator/carbonator.py, it has some modifications to adapt it for our implementation.

A couple more requirements:
* pip install python-owasp-zap-v2 w3af-api-client

To-Do:

To add more tools and to improve the detection of errors of the tools.
We are really looking forward to hear your recommendations, questions and pull requests!

About The Author

Francisco Amato is a researcher and computer security consultant who works in the area of vulnerability Development, blackbox testing and reverse engineering. He is CEO of Infobyte Security Research (Infobyte LLC) www.infobytesec.com, from where he published his developments in audit tools and vulnerabilities in products from companies like Novell, IBM, Sun Microsystems, Apple, Microsoft. Infobyte LLC. founded in 2001, providing specialized services in offensive security, is the first company providing Red Team Services in Latin America. By using real attack scenarios where the physical security and the IT infrastructure of our clients is put to the test. Faraday is the first Multiuser Penetration IDE released back in 2013 by Infobyte LLC http://www.faradaysec.com. Designed for distributing, indexation and analysis of the generated knowledge during the engagement of a penetration test. The main purpose of Faraday is to re-use the tools available in the community to get more advantage from them in a multiuser way. His last work was evilgrade a modular framework that allows the user to take advantage of an upgrade process from different applications, compromising the system by injecting custom payloads.

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

http://twitter.com/famato

CYBER SECURITY EXCHANGE

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

#CYBERXCHANGE

MEET THE SPEAKERS:

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

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

NEAL KIRSCHNER
CISO
Madison Square Garden

JEFF KENNEY
CISO
First Bank

GRAM LUDLOW
Managing Director
Information Risk
Flowers Foods

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

MARC CRUDGINGTON
CISO
Woodforest National Bank

LARRY WHITESIDE JR.
CSO
Lower Colorado River Authority

CHARLES LEBO
CISO
Kindred Healthcare

BROOK CONNER
CISO
Estée Lauder

Beyond the Breach - Where will the next shoe drop?

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

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

BROUGHT TO YOU BY: IQPC Exchange

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

bitglass BlueTalon CENTRIPETAL NETWORKS CYBERSHEATH DARKTRACE IBM NOVETTA

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

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

vs.

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

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

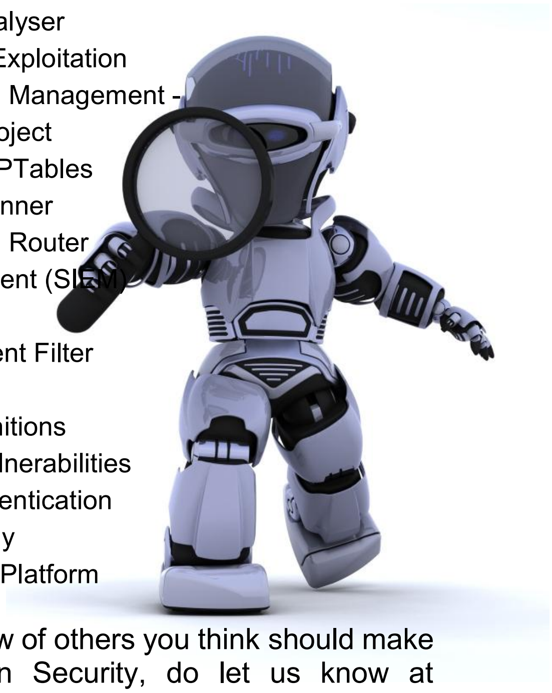
Top Twenty INFOSEC Open Sources

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

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

Here they are:

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



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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

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

So use it by going here:

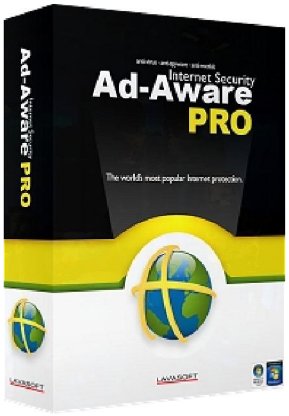
http://www.naisg.org/techtips.asp

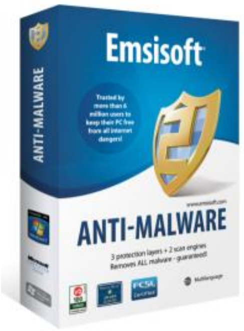
SOURCES: CDM and NAISG.ORG

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

http://register.cyberdefensemagazine.com

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





Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

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

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

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

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine October 2015

Sample Sponsors:

RSA CONFERENCE
StillSecure
PORTCULLIS
Hawk Mobile Monitor
Monitor Mobile Devices Remotely From Your Computer
AFORE
SECURE THE CLOUD. TRUST THE CLOUD.
NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION
CENTER FOR INTERNET SECURITY
Software Developer's JOURNAL
new ideas & solutions for professional programmers
SWIVEL
the power of knowing
SnoopWall
RECLAIM YOUR PRIVACY™
KASPERSKY lab
dekart
MAKE IT SECURE
INFOSEC WORLD
PWNIE EXPRESS
EncrypTight™
BLACK BOX WAN Encryption
GO ANYWHERE™
BLUESPACE
CYBER SECURITY SUMMIT 2014
June 5 DC Metro
Sept. 18 New York City
CYBER INTELLIGENCE USA
18-20 JUNE 2014 - ARLINGTON/V.A
NETWORK MONITORING REDEFINED
See How RSA Security Analytics Detected Heartbleed
Watch video »
RSA
EMC²
INDUSTRIAL CONTROL CYBER SECURITY
OCT 6/7 USA
INDUSTRIAL CONTROL CYBER SECURITY
SEPT 29/30 UK
2nd Annual Privacy, Policy & Technology Summit
January 26-27, 2015 New York
INFOSEC WORLD
Conference & Expo
March 23-25, 2015 | Orlando, FL
January 21–22, 2015 Calgary, AB
Cyber Security for Energy
CYBERTECH 2015
THE EVENT FOR THE CYBER INDUSTRY
The UK Energy Cyber Security Executive Forum
London, 5th February
20% discount (CYSENCDM)
CYBER SECURITY FOR FINANCIAL SERVICES
June 14 - 16, 2015 • Charlotte, NC
THE CYBER SECURITY SHOW
13-14 April 2015
etc venues 155 Bishopsgate, London

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

CDM
Secure Your IT World

CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

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

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS

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

Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for October 2015

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

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

Malware turns hundreds of security cameras into a botnet

http://www.engadget.com/2015/10/25/cctv-camera-botnet/

New strain of malware attempts to entirely replace browser

http://www.scmagazineuk.com/new-strain-of-malware-attempts-to-entirely-replace-browser/article/449285/

'10-second' theoretical hack could jog Fitbits into malware-spreading mode

http://www.theregister.co.uk/2015/10/21/fitbit_hack/

How to Avoid Malware when Downloading and Installing New Software

http://neurogadget.com/2015/10/24/how-to-avoid-malware-when-downloading-and-installing-new-software/18318

Mac malware hit all-time high in 2015

http://bgr.com/2015/10/21/mac-malware-increase-2015/

Cisco offers free help to rid hosting providers of major malware stores

http://www.itworldcanada.com/article/cisco-offers-free-help-to-rid-hosting-providers-of-major-malware-stores/377931

Kickass Torrents Is Infected With So Much Malware It's Starting To Look Like The Pirate Bay

http://www.ibtimes.com/kickass-torrents-infected-so-much-malware-its-starting-look-pirate-bay-2152522

Hackers being hunted after stealing $30.7M via malware

http://www.cnbc.com/2015/10/14/hackers-being-hunted-after-using-dridex-malware-to-steal-over-30m.html

Medical Websites Targeted By 26% Of All Malware In 2015, Digital Assault On Healthcare Ramps Up

http://www.ibtimes.com/medical-websites-targeted-26-all-malware-2015-digital-assault-healthcare-ramps-2150765

Malware Surges in First Half of 2015

http://www.itbusinessedge.com/blogs/data-security/malware-surges-in-first-half-of-2015.html

iPhone Malware Is Hitting China. Let’s Not Be Next

http://www.wired.com/2015/10/iphone-malware-hitting-china-lets-not-next/

The Dark Web Is Becoming a Safe Haven for Malware

http://motherboard.vice.com/read/malware-is-using-the-dark-web-to-stay-hidden

Malvertising: Daily Mail ads 'briefly linked' to malware

http://www.bbc.com/news/technology-34541915

Thousands of e-commerce Magento websites struck with Guruncsite malware

http://www.zdnet.com/article/thousands-of-e-commerce-magento-websites-struck-with-guruncsite-malware/

The Most Dangerous Financial Malware Threats

http://www.lowcards.com/cypher-reveals-dangerous-financial-malware-threats-36987

This vigilante virus protects you against malware attacks, quotes Richard Stallman

http://www.pcworld.com/article/2988933/security/this-vigilante-virus-protects-you-against-malware-attacks-quotes-richard-stallman.html

Android malware apps might net hackers millions, fool Google Play Store security

http://bgr.com/2015/10/15/ghost-push-android-malware-apps/

Attacker slips malware past Ubuntu Phone checks

http://www.theregister.co.uk/2015/10/18/attacker_slips_malware_past_ubuntu_phone_checks/

Apple Officially Addresses YiSpecter iOS Malware Woes: Here's The Deal

http://www.techtimes.com/articles/92151/20151008/apple-officially-addresses-yispecter-ios-malware-woes-heres-the-deal.htm

Heimdal: Malware campaign uses blackhat SEO to deliver malicious code

http://www.scmagazine.com/heimdal-malware-campaign-uses-blackhat-seo-to-deliver-malicious-code/article/448285/

After pushing malware, ad networks also used for DDoS

http://www.computerworld.com/article/2987036/application-security/after-pushing-malware-ad-networks-also-used-for-ddos.html

Ghost Push malware evolves in Android app infection spree

http://www.zdnet.com/article/ghost-push-malware-evolves-in-android-app-infection-spree/

CDM

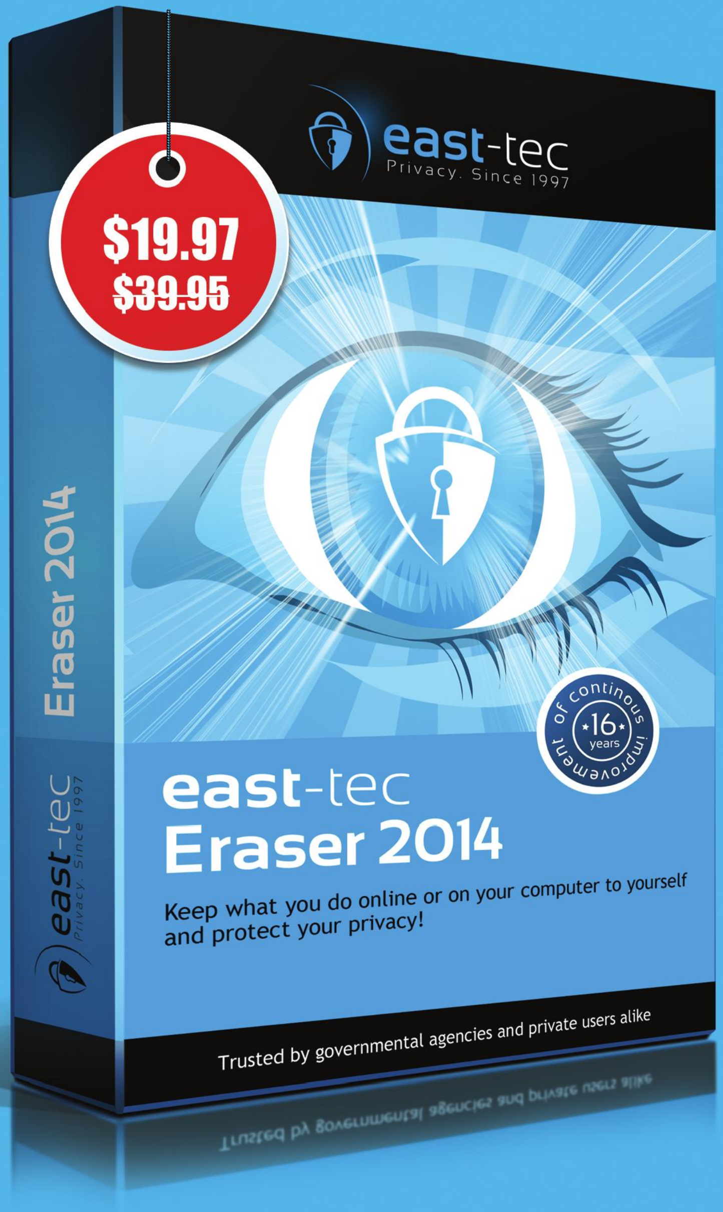
CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

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

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

Cyber Defense Magazine - Cyber Warnings rev. date: 10/28/2015


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