SAMSUNG Knox

White Paper: Mobile Malware and Enterprise Security

August 2016

Samsung Research America
Samsung Electronics Co., Ltd.

SAMSUNG

Contents

SAMSUNG

Acronyms

BYOD	Bring Your Own Device
COPE	Corporate Owned Personally Enabled
DAR	Data-at-Rest
DIT	Data-in-Transit
DIU	Data-in-Use
DoS	Denial of Service
MDM	Mobile Device Management
MitM	Man-in-the-Middle
SE for Android	Security Enhancements for Android
TIMA	TrustZone-based Integrity Measurement Architecture
USRP	Universal Software Radio Peripheral
VPN	Virtual Private Network

Managing the moving target of BYOD

To understand the immediate need for enterprise security solutions, reviewing the history of Bring Your Own Device (BYOD) helps to tell the story of why security is no longer optional.

It was only eight years ago that smartphones entered the market. Employees were already bringing their personal phones to work, but smartphones suddenly allowed access to corporate email, making it easier to respond to work-related demands after work or during business travel. Document sharing was faster and easier, and smartphone calendars made meeting reminders mobile. The BYOD evolution started slowly, then accelerated with the proliferation of apps for every business and personal need. However, IT admins were blindsided with the new and growing problem of protecting corporate intellectual property from the avalanche of unprotected personal property employees brought to work.

The security model used by IT departments was originally designed to protect an enterprise network and company-issued PCs, not the personal smartphones and tablets employees are bringing into the workplace today. With BYOD and cyber attacks both increasing, enterprises must address security with tools to thwart the massive vulnerabilities enterprises face today.

Many enterprises are still not acknowledging the security risks and burdens of IT admins until after the company is hit with a major cyber attack and data is compromised. Malware is familiar territory to IT admins managing an enterprise network, but trying to manage personal smartphones and tablets is an entirely new battleground, and it's an expensive one.

Ponemon and Norse, published a joint report, *Live Threat Intelligence Impact Report 2013*, a study of 378 enterprises with 708 participants. Of the key findings, money tops the list. $10 million is the average amount spent in the past 12 months to resolve the impact of exploits.[1]

$10 million is the average amount spent in 12 months to resolve the impact of exploits.

Live threat intelligence is defined in the Ponemon and Norse report as having access to the most immediate threat intelligence available.[2] IT admins must know how to identify threats, what to look for, and to monitor a network for the unexpected. Sixty percent of respondents said their enterprises were unable to stop threats because of outdated or insufficient threat intelligence.[3] If threat intelligence for monitoring networks is insufficient, where do enterprises stand with monitoring mobile devices that contain sensitive corporate data?

SAMSUNG

Smartphones and apps — is your corporate data at risk?

Portability and connectivity have made smart phones and tablets the devices of choice for social media, streaming videos, and online shopping. Consumers have devices with them 24/7, and use them wherever they are. This *always connected* trend moved into the workforce as well with the advent of BYOD. One device for work and play is what employees prefer. The trend is here to stay, and continues to rise.

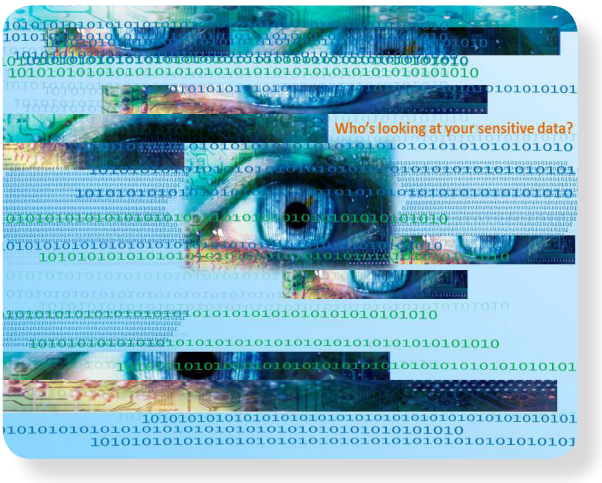
Employees download apps for work and play, but not all apps are regulated. Some third-party apps are known to be designed for malicious use. They can introduce spam, Man-in-the-Middle attacks, and phishing emails. But, it gets worse when you add in unsecured Wi-Fi networks and Trojans that can steal sensitive corporate data.

Smartphone owners spend eighty-six percent of their time using apps versus the mobile web according to the Nielsen February 2014 report, *The Digital Consumer*[4]. That was eighty-six percent last year, and smartphone ownership is growing, as well as the number of apps available. For enterprises using BYOD or a Corporate Owned Personally Enabled (COPE) solution for employees, but with no security solution in place, eighty-six percent of time spent using apps should be an alarming percentage.

IT admins already know the risks that plague corporate PCs and networks, but hackers have designated smartphones as the new frontier to conquer. With so many security risks to juggle, enterprises must adopt a security plan that covers all the bases.

"Eighty-four percent of smartphone and tablet users say they use their devices as second-screens while watching TV."

"Smartphone owners spend eighty-six percent of their time using apps versus the mobile web."



In addition to malware, employees can accidently leak data. Consider another finding from the Nielsen report. Eighty-four percent of smartphone and tablet users say they use their devices as second-screens while watching TV[5].

This spells distraction disaster for employees using their smartphones and tablets for work and play. An employee can send an email or urgently needed sensitive document to the wrong recipient. It's happened many times. Verizon's *2014 Data Breach Investigations Report* says,"Misdelivery (sending paper documents or emails to the wrong recipient) is the most frequently seen error resulting in data disclosure."[6]

SAMSUNG

Security incidents on the rise: What are the numbers?

In 2013 and 2014, the news of malicious attacks on businesses saw hacked Twitter accounts including the Associated Press, The Guardian, The Financial Times, CNN, The Washington Post, Time Magazine, The New York Times, New York Post, and Social Flow.

We also saw attacks on other familiar businesses including Target, Neiman Marcus, Facebook, Evernote, Living Social, Drupal, the Washington State Administrative Office of the Courts, the Federal Reserve internal site, Adobe, Home Depot, JP Morgan Chase, a White House unclassified network, and the one no one will forget—Sony.

Major news stories caught our attention with well-known enterprise names, but the number and types of attacks are staggering. Verizon's *2014 Data Breach Investigations Report* listed 63,437 security incidents in 2013, and 1,367 confirmed data breaches in 95 countries around the world.[7]

The Juniper Networks Mobile Threat Center, a global research facility on mobile security, released its third annual *Mobile Threats Report* in June 2013 from data collected from March 2012 through March 2013. They found mobile malware threats growing at a rapid rate of 614 percent to 276,259 total malicious apps, demonstrating an exponentially higher cyber criminal interest in exploiting mobile devices.[8]

Mobile malware is growing at a rapid rate of 614%

276,259 malicious apps

63,437 security incidents

1,367 confirmed data breaches

With the rising risk of apps designed for malicious intent, and employees demanding BYOD policies, enterprises must adopt a secure end-to-end security solution. IT admins working to protect a network are over-burdened with managing hundreds or thousands of personal mobile devices. Multiply the number of employees by a guess at how many apps reside on each phone, then factor in the 86 percent of time smartphone owners are using apps. But the equation doesn't stop there. Smartphone users are multi-tasking with enterprise data on their personal mobile devices used as a second screen while watching television. Multiply human error by distraction, and add a guess at how many employees are technically aware of how to use their devices and apps. What about Wi-Fi security, third-party vendors, insider threats, and lost devices? The list goes on and on. Managing BYOD by increasing IT resources without a security solution is a stop-gap method at best.

The bottom line is that BYOD is a runaway train that can't be stopped. Every unsecured mobile device connecting to your enterprise is welcoming beacon of light for attackers leading them to all the unlocked doors to your enterprise data.

Mobile malware is a new playground for hackers

For BYOD enterprises, there's no way to know how many personal apps each employee has downloaded, but more apps on a device means the likelihood of app malware is higher. Aspect Security, application security experts, did a random sample of hundreds of applications from organizations including financial, banking, government, defense, ecommerce, transportation, and more. If you weren't worried about apps before now, digest the main message from the *2013 Global Application Security Risk Report*.

98% percent of applications presented at least one application security risk, while the average application registered 22.4 risks.[9]

The report identified, "Authentication and Session Management risks affect 93% of applications and comprise 34% of application vulnerabilities, by far the most prevalent application security risk." [10]

What are the types malware posing threats to smartphones and tablets? The names aren't new. They've been around for a long time threatening PCs and enterprise networks. The ammunition cyber criminals use to attack smartphones include names you've heard before: Man-in-the-middle attacks, Trojans, Viruses, Worms, Spyware, Adware, Botnets, Phishing emails and SMS, Denial of Service (DoS) attacks, Root exploits, and compromised cell towers.

Any BYOD or COPE device that falls prey to cyber criminals and then connects to the enterprise network, can potentially pass on the problem. IT admins know serial numbers of PCs and which employee is assigned to that PC. Without a plan to integrate BYOD devices into your security system, these smartphones and tablets are unidentified and unaccounted for devices connecting to your network.

In addition, data breaches can also occur from accidental errors, insider misuse and lost or stolen devices.

What employees do with their personal devices is personal. Enterprises allowing BYOD cannot control what apps they use, or when they use them. But because smartphones and apps are highly targeted by cyber criminals, it's wise to at least know how devices are being used.

Malware, short for malicious software, comes is many forms, and is used to gain access to private computer systems and networks to steal sensitive information. Mobile devices are also vulnerable and can be used to steal resources (CPU, disk, bandwidth) to distribute more malware or illegal goods.

What can mobile malware do?

The most common source of mobile malware comes from third-party apps users download. Many are unregulated, and contain malware to hijack the phone. Depending on the type of malware, the results can include:

- Hack your email
- Send spam to all your contacts
- Delete files
- Delete images
- Take over use of the camera
- Lock the phone
- Steal data, passwords, PIN numbers
- Listen to phone conversations

Spam sent to your contacts may be the biggest problem of all. These can be phishing emails which look like they are from a trusted contact. But, they direct users to a website that collects information such as usernames, passwords, PIN numbers and other information to gain access to personal information used to steal money or data.

Even the most advanced users aware of security risks can be lured into being fooled by phishing emails.

Adware and spyware

Adware is often bundled with free software and is usually removed if the software is purchased. The advertising constantly running is irritating, but usually not malicious.

Spyware is designed to do just what the name suggests—spy on the device user. On a mobile device, the most common way spyware gains access is through downloaded apps. Online browsing can be tracked, as well as phone usage. Spyware can steal sensitive information such as bank account and credit card information, user logins, and is often difficult to detect.

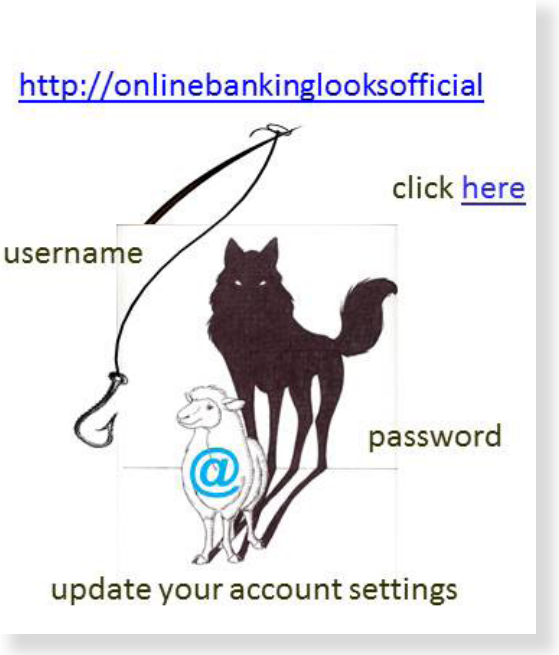
The Knox Workspace container separates enterprise data from personal data, and app whitelisting gives IT admins control over which apps can be downloaded.

Compromised cell towers

Universal Software Radio Peripheral (USRP) radios can be used to intercept cell phone signals. An attacker hijacks a cell phone call, tampers with the routing of the call, and appears to be a legitimate cell phone carrier. When smartphones connect to them, the attacker can listen to phone calls, read text messages, and launch exploits targeting the baseband radio chip on the phone.

A USRP can be used in place of a real cell tower. The attacker must be physically close to the victim to intercept a call. If they want the calls to be correctly routed back to a real tower, the attacker can simply relay them to a real tower that is nearby. All the equipment needed, including the USRP radio, is small enough that the attacker can easily carry it in a car. Not only can they listen to your calls, they can actually answer your outgoing calls.

Email phishing



Phishing is way for hackers to gain access to sensitive data. The attacker is truly a wolf in sheep's clothing, pretending to be a trusted person, a website, or app requesting information. The attacker can send an email or SMS messages containing a link to a malicious website that looks like a trusted site, such as a bank or social networking site. Once the user goes to the fake website, the attacker can infect their device with malware to collect information. Most phishing is done to collect money or sensitive enterprise data or to gain login credentials for other reasons. The number of phishing attempts has increased in the past few years. Very high-profile cases of phishing show that even users with knowledge of malware can become victims. Hackers create website replicas that look extremely convincing.

Enterprises can end up losing sensitive data with just one employee clicking on a fake website. But, hackers can also use that employee's email to find other email addresses within the enterprise to send more phishing emails and gain access to the enterprise network.

Malicious websites

The internet is an integral part of everyday life. Many people use websites for banking, shopping, listening to music, watching videos, watching television, playing games, sharing photos and stories on social media, reading the news, and the list goes on.

The more time we spend online makes the job of cybercriminals easier. They make their living stealing data and money. More websites and more people online equals more financial gain. There are several methods used to get web users to visit malicious websites. Phishing and spam emails entice users to visit what appears to be a legitimate website. Just recently, an email offered a coupon for a free pizza from Pizza Hut because the company was celebrating its 55th anniversary. But clicking on the link delivered malware instead.

Another method is a drive-by threat, sometimes called a drive-by download. Cybercriminals infect a legitimate website, then redirect users to a malicious site that appears to be okay while downloading malware in the background.

Enterprises small, medium and large protect their networks, but too often overlook the smartphones and tablets which have enterprise data left unsecured. This ups the ante for cybercriminals with hundreds or even thousands of devices left with doors wide open.

Man-in-the-middle attacks

Man-in-the-middle (MitM) attacks happen when the MitM, the attacker, intercepts a client and server during the exchange of a public key. The MitM sends his private key instead, and pretends to be the intended client and intended server. For example, Bob, a smartphone user (the client) wants to check company email while traveling. He unknowingly connects to an unencrypted Wi-Fi wireless access point and logs on to his email. Secure Socket Layer (SSL) is always used to make sure the client and server connections trust that they are who they say they are. They must each send a certificate to the other verifying their identity. However, the MitM intercepts between the client and server. He sends his certificate to the server, which accepts it. Then, he sends the client forged proof that he, the MitM, appears to be the server. Now, all Data in Transit (DIT) intended to go between the client Bob and the email server, is actually going from Bob to the MitM to the server. He can eavesdrop on Bob and see if there's data he's interested in. If so, he can steal the data, and then reconnect the actual Bob and the email server. The whole process goes undetected.

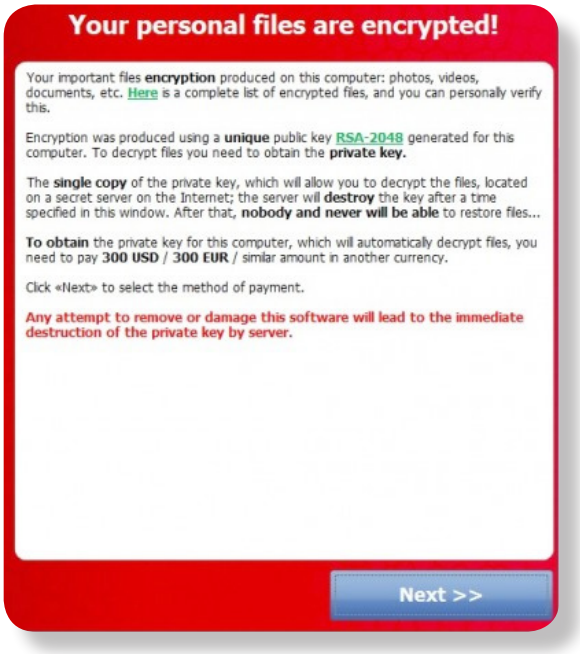
Apps often ignore bad certificates and continue to communicate with untrusted servers. The Knox VPN protects against this by providing a verified encrypted channel to a remote server even over unsecured Wi-Fi networks. Knox Client Certificate Manager (CCM), located inside TrustZone, protects certificates on a device. SSL is another protection designed to protect communication on unencrypted access points.

Root exploits

A rootkit is used maliciously by hackers to maintain root access to a computer or smartphone. Root access is the highest level of control or Administrator access. To understand this type of access, think of when you allowed an IT admin to take over your computer to fix a problem. You temporarily gave control to the Admin, and watched the actions on the screen. Once a hacker gains root privileges, they usually install a rootkit to maintain these privileges and hide activities from the user. These rootkits usually enable the attacker to run malicious payloads, monitoring the user's activities (such as with a keylogger) or using their mobile device to launch further attacks on the enterprise network.

An especially insidious payload enabled by some rootkits involves remote access functionality. By listening for commands from the network, legions of infected devices can be turned into a botnet. These botnets can be used for many malicious purposes, sometimes literally being rented to the highest bidder. The information contained on the devices in the botnet, and the access they enjoy, is part of the package.

Trojans



Trojans (Trojan horses) are a type of malware that look safe or even helpful, but contain malware. A common example is fake anti-virus software. The site looks real, but is actually installing malware.

The name Trojan horse comes from Greek mythology where the Greeks won the Trojan war by sending a gift horse to the Trojans that actually had soldiers hiding inside. The Trojan priest warned to beware of Greeks bearing gifts. Downloaded apps may also bear malware gifts, and are rarely detected. A Trojan can take remote control of a computer or smart device and can download or upload files, delete files, modify files, encrypt files, and steal data and passwords. Once files are encrypted, a hacker offers to unencrypt the files for a ransomware fee. Apps are the most common way Trojans are introduced to mobile devices. Re-packaged apps that appear to be a familiar app have turned out to be Trojans on smartphones and devices.

In 2007, the Trojan Zeus was discovered after compromising online banking, social networks and email accounts. There are many well-known variations of Zeus that have been found on mobile devices.

SAMSUNG

Viruses and worms

Viruses and worms are both malware that attach to software programs and can reproduce and spread each time the software is used. For example, a virus or worm can attach to a spreadsheet program. They are often introduced by email, and can spread to other devices through the list of email contacts.

The term worm comes from the way the malware spreads through holes found in security networks. Worms differ from viruses because they don't have to attach to software programs. Worms can encrypt files, delete files, or send email attachments. The ultimate goal is to spread to as many other devices as possible.

One of the most famous worms, Stuxnet, was discovered in 2010, and has been called one of the most sophisticated exploits in history. The worm started by infecting a system via a USB stick with fake digital certificates that appeared legitimate. Stuxnet then checked for PCs running a control system made by Siemens which ran high-speed centrifuges in Iranian nuclear plants. When those were found, Stuxnet connected to the internet and downloaded new versions of itself. The worm then exploited zero-day software attacks to take control of the system and learned how to make the centrifuges spin until they failed. It was also able to send false information to controllers, so that no one could figure out what was causing the failure.

There are analogous viruses that have been found on smartphones that read contacts and send text messages to them. The messages contain a link to an exploit, which then sends the same message to all the contacts found in each device. This quickly replicates and spreads to many devices. However, with the Knox container, business contacts cannot be exploited when the MDM policy to share contacts is turned off.

Samsung Knox™ Security solution

Looking at all the types of mobile malware sheds light on the many problems enterprises face. But more important is finding a solution to protecting your enterprise. Samsung Knox entered the market in 2013 and continues to evolve to protect enterprises and their data, while providing employees with the productivity needs of BYOD.

The Samsung Knox security solution is designed to be the most comprehensively secure and manageable mobile device solution for enterprises large and small. The foundation of Knox is device security rooted in fixed hardware mechanisms. This foundation is based on the principles of trusted computing, a set of methods for making devices that can prove to enterprises that they are running the correct security software, and can raise alerts in the event that tampering is detected.

On top of this trusted foundation, Knox builds a Workspace environment to protect enterprise apps and their data, a robust set of Data-at-Rest protections, and a large suite of enterprise security tools, including a highly configurable Virtual Private Network (VPN) and Mobile Device Management (MDM) interfaces.

Knox Workspace offers a defense-grade, dual-persona container product designed to separate, isolate, encrypt, and protect work data from attackers. This work/play environment ensures work data and personal data are separated and that only the work container can be managed by the enterprise. Personal information such as photos and messages are not managed or controlled by the IT department. Once activated, the Knox Workspace product is tightly integrated into the Knox platform.

For detailed information on the Knox Security Solution, see the whitepaper *Samsung Knox™ Security Solution* and *An Overview of the Samsung Knox™ Platform*. Both whitepapers are available on the Knox website: www.samsungknox.com

SAMSUNG

Endnotes

[1] Ponemon Institute, *2013 Cost of Cyber Crime Study: United States*, October 2013, p. 4. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[2] Ibid, 12.

[3] Ibid, 4.

[4] Nielsen, *The Digital Consumer*, October 2013, p. 8. http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/the-digital-consumer-report-feb-2014.pdf

[5] Ibid, 14.

[6] Verizon, "2014 Data Breach Investigations Report," p. 29. https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf

[7] Ibid, 2.

[8] Juniper Networks, "Juniper Networks Third Annual Mobile Threats Report, March 2012 through March 2013," p. 4-6. http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

[9] Aspect Security, Inc., "2013 Global Application Security Risk Report," p. 1. http://cdn2.hubspot.net/hub/315719/file-681702349-pdf/presentations/Aspect-2013-Global-AppSec-Risk-Report.pdf

[10] Ibid.

Mobile Malware and Enterprise Security	V_1.4	August 1, 2016
Mobile Malware and Enterprise Security	V_1.3	November 12, 2015
Mobile Malware and Enterprise Security	V_1.2	May 11, 2015

SAMSUNG

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales exceeding KRW 201 trillion.

To discover more, please visit www.samsung.com

For more information about Samsung Knox, visit www.samsung.com/Knox

Samsung Electronics Co., Ltd.
416, Maetan 3-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772, Korea

SAMSUNG