Mobile Malware in the Enterprise

Stephen Garrett Allen
12/7/2015

Abstract

In today's enterprise bring your own device or BYOD is prevalent and mobile malware is maturing out of its infancy stage. To combat these threats we can align the business with best practices and standards by using current strategies in diagnosing and defending against malware on personal computers. There are many mobile devices but I will discuss IPhone and Android in this paper to narrow the topic. Staying on top of new advanced threats and helping your employees secure their personal mobile device in their everyday life will ensure the device is protected when connecting to your enterprise network. I will discuss the three types of mobile malware PUS, ransomware, and information leakage. By providing your employees with Security Training Awareness you can help reduce potential threats brought into the company. I will discuss topics to cover while training your employees and what methods are being used now. Staying up to date on the latest news and part of mobile security community are going to be another great way to stay informed.

Mobile Security Paper
Mobile Malware in the Enterprise
Stephen Allen
12/7/2015

With enterprise businesses spending more than ever to defend against external advanced persistent threats we need to be secure against internal threats as well. As previously mention these insider threats might not be intentional but can do significant damage. With malware infecting a personal device and that device connection to your enterprise can WAN/LAN the attack may be able to use escalation of privilege or move laterally inside your network. By providing your employees with a Security Training Awareness, the right mobile tools and constantly enforcing an open door security policy. For your security team it will be an ongoing battle to constantly review the mobile security policy and to keep a balance with your employees by allowing them to continue to use the personal devices on your enterprise network. By using Mobile Device Management software and Unified Threat Management software just as in other sectors of computing which are becoming more software defined.

Whether it's iOS, Android or Windows Phone, you can enable the end users in your organization to be more productive and secure on the go by supporting the smartphones and tablets they use on a daily basis. Email is the main use for mobile phones and in some cases these communications contain sensitive corporate information. The majority of enterprise is on MS Exchange for corporate email use which they host onsite or in the cloud. Right now most enterprises have some type of BYOD policy enforced using a hybrid of enterprise software and hardware to manage their employees mobile devises at work.

By adding enterprise mobility it empowers the employees to be more productive all the time in any location. With this brings a new set of security issues from business data leakage and access to the cooperate network via VPN from remote unsecured locations. When technologies mediums shift via manufacture or platform or for example from pc to mobile the bad guys are able to quickly able to target the new system. Mobile Malware is on the rise but with proper enterprise level security solutions deployed and enforcing BYOD with a mobile enterprise policy you can be successful in protecting your network. “These elements enable

software defined environments to achieve agility, efficiency, and continuous outcome-optimized provisioning and management, plus continuous assurance for resiliency and security." (*Li, C., and BL Brech)

There are some strong stances you will have to take such as restricting the types of mobile devices or application that our permitted on your network. In the enterprise you should restrict the type of mobiles devices or applications that are allowed to join your network. For example an employee with an outdated android device that is no longer being updated may have system vulnerabilities that are hard to protect against.
A look back at 2015 shows that malware didn't rise in volume but matured in nature of the type of malware attacks which now include ransomware and stealthy insertion of spyware. Some interesting points of the article is that users still rarely get infected but typical actions that lead to an increase in the change of infection are number one jailbreaking the device. The second is pornography sites which trick the user into installing video players, codecs, or other forms of software. The most successful mobile malware tactics still includes phishing attacks including spear phishing which specifically targets the user by using social engineering tactics states the Blue Coast Systems 2015 Mobile Malware Security Report.

Further in the report is helps explain about emerging threats that now mobile application are polymorphic binary files. When downloaded the file creates the app with 99% of the code and adds a small piece of junk data to the end that helps the newly created file slip past signatures based detection and researchers. This also make it difficult to count the exact type of malware in an enterprise or in the wild because there can be many different variants of the same exact malware program but takes time to disassemble and test each piece of malware data program. One malware type identified in the report is Potentially Unwanted Software or PUS-infected which could use SMS messaging to sign up for junk that does cost real money applied to your carrier phone bill or siphon the data from your contract list. The caveat of this is that PUS will not steal credit card numbers, emails, or your banking creditable which in the workplace could be administrative login credentials, or VPN.

The second type of malware is ransomware, which usually encrypts music files, photographs, videos and other documents while demanding bitcoin. In the recent past it has been known to add a timer and state it will permanently erase the files if the payment is not met by the deadline to increase the percentage of payments.

Ways to prevent this in the enterprise is to have backup software, and mainly anti-ransomware software running which is included in new Unified Threat Management systems. Most of the smartphone encryption can be broken in the hands of an expert, but some are starting to use true AES encryption with a time limit starting once the encryption starts. It doesn't give the security expert any option other than to wipe the device and reload. This is another reason to have a preapproved enterprise application store and advise your employees to use it and if they do have any questions to ask the IT department to approve or make a suggestion. Most of the ransomware is installed because users installed cheap, often free or pirated applications on the mobile device.

Information Leakage from applications poses another security risk for the enterprise on a daily basis. Often the applications developers don't encrypt the data and the user has no system utility to view what information is being leaked. Usually the information leakage will show the operating system, the manufacture, the specific app or browsers being used. Sometimes information can be sent back to advertisers, web statistics firms, or other unknown third parties. Figure 1 below shows a type infection cycle for mobile devices.

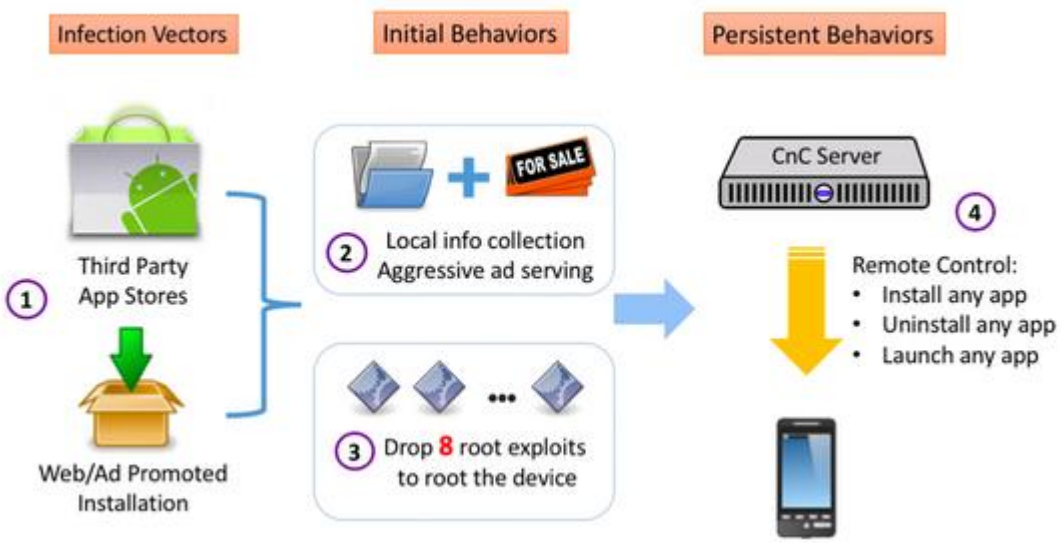

Figure 1.

By using social engineering, the number one way for a hacker to infect a specific target is to convince them to install a malicious app and approve the controls and now a mobile Trojan can be uploaded. The report states "a number of vulnerabilities in Android and iOS were revealed in the past year which may give hostile

third parties the ability to force our devices to infect themselves without our will assistance." While Apple and Google have been working on updating their OS'es, the mobile phone providers does have a lot to consider before pushing down "over-the-air" updates and some phones which are a year or more older are often not updated by OTA. This requires novice phone users to understand how to browse the manufactures mobile phone site and download OS and possibly firmware updates and then complete an install successfully. This can often prove difficult for an average user and possibly even been a bigger issues with a tech savvy user who downloads or installs a trojanized version of the OS or firmware from a torrent.

The 2015 Mobile Malware Report also states that pornography sites are back on top as hosting malvertisting attacks and sites which host Trojan horse app that trick the porn site visitor into downloading and installing. The most common Trojan app install method being requested is to install a specific codec or video player. On iOS and Android users can use the press and hold technique to reveal the true url of a short or tiny url link. Some steps you can take are to invest in a mobile device management software for greater visibility, enable a guest Wi-Fi with policies around data access and allow employees and guest access.

We are just starting to see content management become a huge area involving data security. If you can get a handle on it now and understand that it is evolving you can stay ahead of the curve. "You can also ensure the integrity of information by use of encryption and DLP technology. Be sure to require or provide an antivirus or full security program and enforce complex password protection for all mobile devices including tablets." (Galen Gruman)

It is most important to practice and ensure the employee exit plan is working and tested regularly. Most data breaches occur after a technical employee has left and it still upset about what happened. Old backdoors and passwords that have not been rotated provide an easy way for an ex-employee to conduct bad behavior. According to a new report from mobile application security vendors Checkmarx and AppSec Labs, the average mobile app has nine vulnerabilities. Of the iOS vulnerabilities, 40 percent were critical or high severity, compared to 36 percent of the Android vulnerabilities, said Amit Ashbel, product marketing manager at Checkmarx.

For the past few years we have seen enterprise deploy a variety of software and hardware based security systems, with the complexity it's added the need for new employees, new training, and possibly vendor setup

support. The enterprise has been looking for a solution and vendors like Cisco and IBM have moved toward a single security solution, one single piece of software that manages every aspect of mobile security. The benefit of UTM is having one company for support, upgrades, and hardware replacement. Mass360, an IBM mobile unified threat management solution, which gives an overview of the entire mobile enterprise system. Mass360 can also enforce a policy where only enterprise approved applications are allowed to be installed on the phone or mobile device. At this time you would need to test and approve each third party app that is requested to be installed. One option is to build your own enterprise apps for use with the company and distribute via the enterprise app store. In this store you can add basic pre approve third party android or IOS apps. Again there could be zero day flaws that are discovered and provided an attack service to the enterprise so it is best to not allow any third party applications. Work with your employees about what they need the application for and find out if there is another productive way to meet their needs. In the future I see a request and build policy where the in house developers will produce apps and release to employees.

Today in the enterprise we have three different options when embracing the new mobile workforce. Though my research I've gathered three different avenues for bring your own device which can be phones, tablets, or other smart devices. First, you can provide each employee with an enterprise mobile device which depending on the size of your business can get expensive. For smaller business may be a valid solution as with most carries they provide a business deal with a contract. This way you can install and enforce the applications and policies at all times and control this device. Secondly, you can allow the employees to bring any device to work and apply a security policy enforcement program and have them agree that this only effects people at work. Third you can allow an open policy and any device an employee bring in can be connected which is not recommended. This may be applied is a situation where the enterprise may not have data online. For example even though they provide a secure email solution in the cloud they don't have a VPN or other common forms of employee access and therefore would not pose a threat.

Do not make assumptions about the manufactures security and that they are protecting the user. We know that Android will put out security updates but the carriers will often get these at a later date. Then it will take time, often weeks, to roll out the update to end users in phases because of the high volume of android phone who either need a security update or an entire system update. One such example was "Stagefright" vulnerability in Android devices. By creating a specially created MMS message the attack could compromise the victim with self-installing malware. One step to avoid this was to turn off auto MMS downloads and same with phishing emails it to not open or click on attachments from unknown users. "The most common vulnerability, which accounted for 27 percent of all vulnerabilities found, was leakage of personal or sensitive information. Authentication and authorization problems were in second place at 23 percent, followed by configuration management at 16 percent. Other vulnerabilities included availability, cryptography weaknesses, disclosure of technical information such as application logs, and input validation handling.
Authentication and authorization vulnerabilities were also the riskiest, with 60 percent of these vulnerabilities ranked as critical or high severity."

The best idea is to start now and get a head start of training with users or at this point to catch up with your mobile policy. Explain how they would feel if banking, social, or personal information was stolen from their phone and segway into corporate data. Under some policies users may be held liable for not reporting stolen or lost electronic devices and you need to take this time to encourage them to do so. Not only will this decrease the amount of a time a hacker has to get information of the device he could be using the compromised accounts to start another attack inside the enterprise network. Employees need to notify the security officer so a remote lock and wipe can be issued, possibly enable geo-location or tracking of the device in a high profile situation where the device was stolen. At the same time you can monitor or lock all possible compromised accounts that deal with the specific attack. You can train your users in the monthly Security Education Training Awareness which can be meetings, newsletters, or memos. Include information about not downloading apps from any unofficial sources and encourage them to request for IT to approve or suggest an application that they think is more secure. Explain to the user do not under any circumstance jailbreak the phone by installing CGYWIN or other custom firmware's as these might be trojanized itself and loaded at boot time. Understand

the risk of connecting to free or unsecure public Wi-Fi networks and that they need to use VPN or an encryption service if using corporate email.

In the paper, A study on the Security Technology of Enterprise mobile information systems he points out that users can always use their mobile 3G/4G access to get past enterprise security. A user could turn of Wi-Fi and then use their mobile service which can sometimes be downgraded to 3G which is un-encrypted and does not have digital signatures. This is another training awareness to make sure when using the corporate network or email to use the secured Wi-Fi access. *Yun, Deng, and Cheng Xiao-hui

Enterprise Mobility Management (EMM) helps you save time and reduce stress when securing, monitoring and managing mobile devices, docs and apps in your mobile environment - and with MaaS360, the setup only takes minutes! MaaS360 by Fiberlink an IBM Company In the near future IBM will release a Crypto Express5S which is a versatile solution for secure computing infrastructure.

As Arnold states “This is done in a way that allows the sensitive key material never to be exposed outside the physical secure boundary in a clear format.” (*Arnold, T.W)

In Authors paper he proposes a new adoption of a network security solution for mobile devices.

“Security in the current environment (with the problems highlighted in Figure 2) mirrors the distributed nature of computing. Endpoint security includes frequent patches for security vulnerabilities and endpoint-based security such as anti-virus, anti-spyware, host intrusion prevention, and host-based firewall.” * **De Los Reyes, G)**

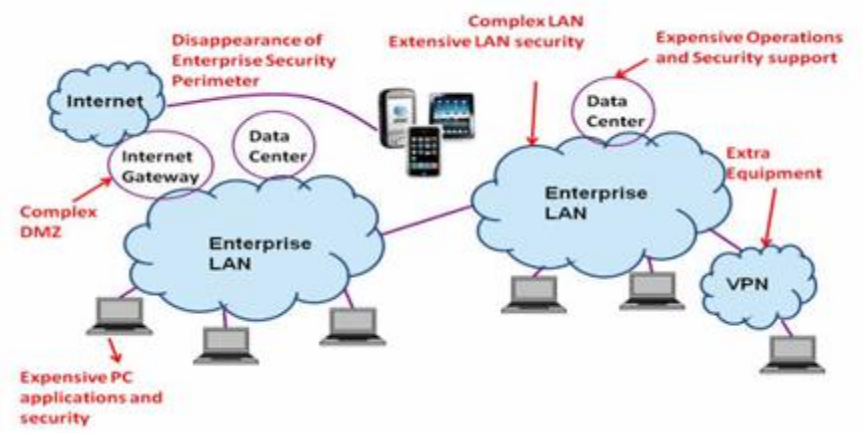

Figure 2.

In the future I see an enterprise landscape regulated by mobile device management software to manage every security aspect for mobile devices. As the threats continue to evolve and more social engineering tactics are deployed aim at our employees have this type of control will be the only way to manage emerging threats. By using a combination of mobile security polices, approved enterprise app store, and continuing mobile security education awareness training for employees will ensure business continues to thrive and is secure. The best method is to embrace this new technology and at the same time make your employees more connected and know your information is secure at all times. If you do not you could possibly have employees who bypass these polices and at a tech company they may be even more savvy. Also they might install bad software unknowingly and will result in a security breach.

Ultimately, you want to empower your technology managers to own the process. Soon you will find that your organization's network will be more secure and your employees will be more productive and happy." (Global Scape PDF)

By enforcing polices and in combination with a mobile device management software suite you can ensure the success of your enterprise mobile security. For now by using a combination of a unified threat management system and enforcing BYOD polices you can be successful and secure in your business.

WORKS CITED

*Arnold, T.W. "The next Generation of Highly Reliable and Secure Encryption for the IBM Z13." IBM Journal of Research and Development59.4/5 (2015): 6:1-:13. Print.

* De Los Reyes, G., S. Macwan, D. Chawla, and C. Serban. "Securing the Mobile Enterprise with Network-based Security and Cloud Computing."Sarnoff Symposium (SARNOFF), 2012 35th IEEE 978-1-4673-1465-7.12821724 (2012): 1-5. Print.

Global Scape PDF https://www.globalscape.com/ Nov 18th, 2015

InfoWorld | Feb 10, 2015 Galen Gruman http://www.infoworld.com/author/Galen-Gruman/ Dec 1, 2015

*Li, C., and BL Brech. "Software Defined Environments: An Introduction."IBM Journal of Research and Development 58.2/3 (2014): 1:1-:11. Print.

Systems, Blue Coat. "2015 Mobile Malware Report." 2015: 12. Print.
http://dc.bluecoat.com/Mobile_Malware_Report

*Yun, Deng, and Cheng Xiao-hui. "A Study on the Security Technology of Enterprise Mobile Information System." Computational Intelligence and Security, 2009. CIS '09. International Conference on 2 (2009): 385-91. Print.

Figure 1.IMAGE is from ---- http://www.csoonline.com/article/2990480/mobile-security/android-malware-hammers-phones-with unwantedads.html?phint=newt%3Dcso_update&phint=idg_eid%3Da355a6e9f9de36f738afa8aa51da3cc6#tk.CSONLE_nlt_update_2015-10-11&siteid=&phint=tpcs%3D&phint=idg_eid%3Da355a6e9f9de36f738afa8aa51da3cc6

Figure 2 IMAGE is from **De Los Reyes, G)** Securing the Mobile Enterprise with Network-based Security and Cloud Computing."Sarnoff Symposium