Mobile Malware

By

Cameron Meyer

Submitted to the Department of Technology Systems

In partial fulfillment of the requirements for the degree of

Master of Science

at

EAST CAROLINA UNIVERSITY

July 2015

This page intentionally left blank

Abstract

Mobile devices with networking capabilities are continuously increasing and users are utilizing these capabilities more. Just like traditional desktop and laptop computers, these mobile devices are vulnerable to attacks from hackers, viruses and other malware. As a result, mobile devices are being targeted by hackers, viruses and other malware entities at an alarming rate. The evolution of this malware has been rapid throughout its short lifespan thus far. This makes protection of mobile devices and preventing attacks and malicious programs imperative. The features of mobile devices allows them to function similarly to desktop and laptop computers and the information on them and transported by them must be protected with equal diligence.

This page intentionally left blank

Table of Contents

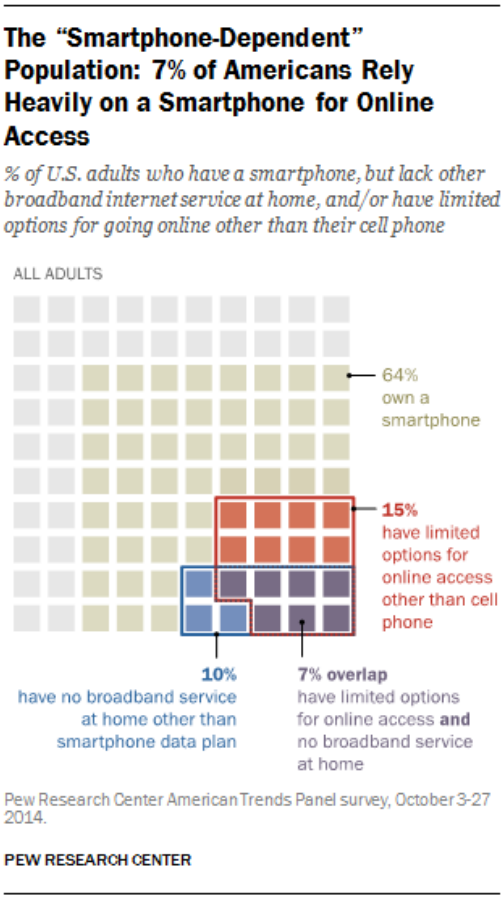
Introduction

Since their invention, mobile devices have evolved and increased exponentially. Today, smartphones and tablets are commonplace for the average consumer. These smartphones and tablets have capabilities similar to traditional desktop and laptop computers in many respects. Consumers use these devices in a broad range of ways but connecting to the Internet is one of the most prevalent. With the ability to connect to the Internet and perform a wide variety of tasks, these mobile devices are being targeted by cybercriminals through the use of mobile malware. This malware can target specific apps or services with the intent to steal information from the use. Mobile malware is any virus or other malicious software that is specifically aimed at mobile devices according to Mcafee Inc. (McAfee, 2011).

Smartphones and tablets have come to dominate the market share of mobile devices in recent years, with over one billion units sold in the fourth quarter of 2014 alone (Gartner Inc., 2015). There are a handful of big players who offer different platforms and operating systems within this category of mobile devices. The largest players are iOS operating system, the Android operating system, SymbOS and J2ME operating systems. These operating system are largely targeted by mobile malware based off of their respective market share and ease to attack. The Android operating system, owning the largest percentage of the market share (Gartner Inc., 2015), is the most highly targeted operating system of all smartphones by mobile malware (Kaspersky, 2013). The next most targeted operating system is the J2ME operating system followed by SymbOS and then all other operating systems (Kaspersky, 2013).

The sale of smartphones has skyrocketed in recent years and according to Gartner Incorporated, sales went up 42.3 percent from 2012 to 2013 and totaled 968 million for the year in 2013 (Rivera and van der Meulen, 2013). In total 64 percent of Americans own a smartphone

in 2015 which is a major increase from 35 percent in 2011 according to Aaron Smith of the Pew Research Center (Smith, 2015). These smartphones are not being used solely for the purposes of texting and making calls but for their higher functioning capabilities such as email, banking and web browsing. Smith goes on to highlight the extent of how smartphones are being used in America and includes the following passage and chart: "In all, one-in-five American adults (19 percent) indicate that at least one of those conditions apply to them, and 7 percent of the public says that *both* of these conditions apply — that is, they do not have broadband access at home, and also have relatively few options for getting online other than their cell phone."(Smith, 2015).



With the number of smartphones and other mobile devices increasing in this manner and their usage on the Internet also increasing, it follows that these devices are being targeted by

hackers, viruses and other malicious programs at an increasing rate as well. Mobile malware has increased dramatically with a growth of 167 percent from 2013 to 2014 according to Kate Vinton of Forbes (Vinton, 2014). There are new threats and variations of attacks constantly being created that threaten users' mobile devices and the information on them via their apps and other services that they provide. As a result, the protection of these assets must grow and evolve as equally in order for their proper safeguard and the information that they carry and transmit to be assured.

Malware Stats

Mobile malware has existed for over a decade since 2004 when the first instance of malware specifically targeting mobile devices was documented. The first mobile malware program was a mobile worm whose target was the Nokia Series 60 phone. The worm flashed the word "Caribe" across the phone screen and then overtook the phone's Bluetooth system to infect other devices in close proximity to the phone (Aprville, 2014). This was accomplished utilizing Short Message Service messaging services on the phone. In 2005 a new malware was discovered that exploited Multimedia Messaging Service messaging services on mobile Devices. This malware came in the form a virus name "CommWarrior" which targeted the contacts on a the phones it infected and sent back the information of those contacts, allowing itself to propagate the infected multimedia message to all the contacts on the original target phone (Aprville, 2014). This incurred a cost upon mobile device users who were infected as the carrier charged for these messages at the time. In 2006 the first major Trojan virus surfaced named "RedBrowser" which presented itself through the Java service in the Internet browser and tricked users by advertising that use of Wireless Application Protocol websites would be easier. Axelle Apvrille of Fortinet described the intent behind RedBrowser as such: "By targeting Java, which was universally supported, rather than the device's operating system, the trojan's developers were able to target a much larger audience" (Aprville, 2014). Throughout 2007-2009 mobile malware evolved little by little but the next major breakthrough in malicious software didn't come until 2010. 2010 saw famous PC malware programs become adapted to mobile device platforms as well as the first botnet, which was targeted at the Android operating system (Apvrille, 2014). A botnet comprised of mobile devices can be even more dangerous and volatile than a botnet of traditional computers because as noted in the 2013 Kaspersky Security Bulletin, mobile devices are turned off much

more rarely than their traditional computer counterparts (Kaspersky, 2013). The next year (2011) witnessed a continuance of targeting the Android operating system with the discovery an adware virus named Plankton that went on to infect over 5 million mobile devices (Apvrille, 2014). In addition to this, one of the most powerful mobile viruses was discovered in 2011. It was named "DroidKungFu" and it enable the hacker to become the administrator of a phone and use its resources without the owner's consent or knowledge (Apvrille, 2014). The year 2013 saw even more development in the mobile malware technology world with the biggest advancement being the discovery a program named "Chuli". Chuli was an Android malware that became a cyber-espionage tool that was able to get into the targeted device via email and then was able to record information such as messages, contacts, location and phone calls and then transmit this information to a remote server (Apvrille, 2014). This kind of tool in the mobile malware world is incredibly dangerous as it can be used to steal sensitive information from political leaders and key personnel of companies for example.

Mobile malware is continuing to grow just as quickly as it has evolved throughout its life thus far. The most commonly targeted operating system by mobile malware programs is the Andriod Operating System as noted by the 2012 Kaspersky Security Bulletin (Zaki et al, 2013). Android continues to be the most targeted operating system because of its ease for cybercriminals as noted in the 2013 Kaspersky Security Bulletin, "it's widely-used, it's easy to develop for and people using Android devices are able to download programs (including malware) from wherever they choose" (Kaspersky, 2013). Mobile malware has grown in number, in 2013 there were 104,421 new mobile malware programs (Kaspersky, 2013). This growth continued into 2014 as there were 295,539 new mobile malware programs created in the year. According to Trend Labs, the total number of mobile malware programs that target

Android operating systems was estimated to be at 718,000 during the second quarter of 2013 (Penning et al, 2014). In addition to this, according to F-Securethere were 259 new threat families and variations to pre-existing families that were learned in the third quarter of 2013 and of those 259 new threats and variations, 252 of them specifically targeted the Android operating systems (Penning et al, 2014).

As noted earlier, mobile malware is constantly evolving. There are many different techniques and strategies that are employed to attack mobile devices. Among the most prominent types of malicious software programs are Trojans, botnet programs, backdoors and adware (Kaspersky, 2013). Trojan viruses have become highly specialized to attack mobile device users' banking apps in an attempt to steal money and or valuable information. There were nine times as many "Mobile Banking Trojans" observed by Kaspersky Labs in 2014 than there were in 2013 (Garnaeva et al, 2014). In addition to malware growing in number and complexity, the last several years has also seen mobile malware become a worldwide issue. In the early stages of mobile malware, the various technologies were geographically isolated. For example, a particular malware virus such as Yxes was isolated within Asia and had no reported cases of infection in the western hemisphere (Apvrille, 2014).

Malware Detection and Prevention

Mobile devices, namely smartphones and tablets have gained so much popularity and been able to dominate the market as thoroughly as they have because they offer a wide array of capabilities similar to traditional computers. However, these mobile devices are also unique from their computer counterparts. Mobile devices are unique due to their "multiple-entrance open system, platform-oriented, central data management, vulnerability to theft and loss" (Penning et al, 2014). Mobile malware has many avenues of approach to get into your mobile device and affect it. Many of the malicious software programs gain entry through the user being careless or unknowledgeable about their device and the potential for it to be attacked. Upon gaining access to a user's mobile device the malicious program has a specific goal to achieve. The malicious program will attempt to escalate its privileges, establish remote control, collect various information and attack financially according to Penning et al (Penning et al, 2014).

Due to mobile devices being used as widely as they are and their capabilities being utilized to carry out important tasks such as finances, these devices need to be protected against all the various attacks that seek to exploit their weaknesses. Detecting malware on a mobile device is the first step towards the protection of a mobile device. A research group from North Carolina State University analyzed the top twenty permissions being requested from a sample of 1260 malware programs and then compared to the top twenty permissions being requested by twenty popular apps. This research group found that the permissions that are typically requested the most by malicious software programs from their sample are the Short Message Service, contacts lists and settings. The Short Message Service permissions that were targeted were: "READ_SMS, WRITE_SMS, RECEIVE_SMS and SEND_SMS". Upon comparing the permissions being requested between the two different groups, the researchers found that the

permissions being requested by the malicious programs were nowhere in the top twenty of the permissions being requested by the apps; thus bringing the researchers to the conclusion that these permissions were requested with malicious intent (Zhou et al, 2012). Knowing what permissions are and how to look for them is a very useful way to help safeguard mobile devices. The permissions requested by malicious programs in the study by Zhou et al give a great start of what to cognizant of when downloading applications from the application marketplaces offered by operating systems.

There are several different techniques that can be employed to detect malware on a mobile device. The first, most basic and most crucial technique that a mobile device user needs to properly protect a mobile device is awareness. The following techniques are discussed by Penning et al: signature-based detection, Google Play Store (Bouncer), the manufacture of built-in-security and security awareness training. Signature-based detection is similar to that of anti-virus software for computers in that it attempts to stop the installation of known malicious apps and threats. Signature-based detection is able to stop and prevent known malware however, its weakness is that it cannot stop apps and threats from being installed that are knew or unrecognized by the software. Google has attempted to stop malware before it even reaches its app marketplace, the Google Play Store with a program called Bouncer. The Bouncer's purpose is to scan all new apps that are attempting to be released on the market for mobile malware. Bouncer also looks at the permissions being requested by apps looking specifically if they request short message service permissions and where these apps will be sending and receiving short message service messages from. The shortfall of the Google Play Store Bouncer program is that it only does this with this specific app marketplace which is typically found on Android operating systems (although Android is the most targeted operating system) and doesn't help

third party app marketplaces or those utilized by other operating systems. Manufacturer built-in security can make a big difference in the security of a mobile device, for example the SamsungKNOX security system on Samsung phones. Samsung has released a built-in security system with their newer smartphones on the Android operating system. SamsungKNOX monitors several areas of operation within the devices. One of the ways it protects the device is that it only allows verified and authorized legal software to run on the device. This security system also analyzes the boot loading process of the device for any tampering and will automatically turn the device off if any tampering with the boot loader has occurred. In addition to this, the security system creates a security container that houses data in order to protect against data leakage. The SamsungKNOX built-in security system is thorough and a very useful tool in securing and protecting Samsung phones although, creating a security container to protect data from data leakage may do just the opposite. If a malicious attack does get around the security system and into the container, the device has essentially yielded all of its most important data. Security awareness training could be the most useful as the user will become more knowledgeable about the proper functioning of the device and be able to spot abnormalities in its behavior and begin a course of corrective action. In addition, these users will be more wary of the apps and other items that are downloaded to their mobile devices (Penning et al, 2014).

Conclusions

Since the emergence of mobile devices, smartphones and tablets have come to dominate the mobile device market. Mobile malware first emerged in 2004 and since that time both mobile devices and mobile malware have grown in number and evolved technologically. Mobile malware has expanded from worms to viruses to adware and the ability to create mobile botnets.

Mobile malware takes several avenues of approach in order to infiltrate a mobile device whether it is through SMS messages, apps that are downloaded or through the web browser. These malicious programs and apps typically take aim at hurting a user financially by stealing vital information or inflicting carrier charges by use of SMS and MMS messages. The vast majority of these malicious apps and programs target smartphones that utilize that Android operating system due to it being the most used platform on the market and its ease to attack.

Security awareness on behalf of the user may be the most influential factor in the protection of mobile devices. The fact is that all the security tools on the market will only slow down the intrusion of malicious programs if the user is not sensible in the use of the device. Security software becomes out of date and needs updating when new threats are discovered. If the user is knowledgeable and sensible and careful about what apps are downloaded, the source that apps are downloaded from, understands basic permissions, etc. Technology is always evolving on both sides such as the integration of the new HTML5 which will also bring about new exploitations from malicious programs (Jones, 2014).

Mobile device users should install anti-virus software with signature-based detection in order to help protect their mobile devices. However, this software will become obsolete if the user does not update it when new updates are available. If a user has a mobile device with the

Android operating system, that user should utilize the Google Play Store when downloading apps as these apps are scanned and analyzed prior to being available on the marketplace. These simple steps and tools can help to protect a user's mobile device from malicious attacks.

References

Apvrille, A. (2014). The evolution of mobile malware. *Computer Fraud & Security,* 18-20. Retrieved July 2, 2015, from ACM Digital Library.

Jones, N. (2014, February 12). Top 10 mobile technologies and capabilities for 2015 and 2016. Retrieved July 12, 2015. https://www.gartner.com/doc/2665315/top--mobile-technologies-capabilities

Smith, A. (2015, April 1). U.S. smartphone use in 2015. Retrieved June 25, 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Rivera, J., & Van der Meulen, R. (2014, February 13). Gartner says smartphone sales surpassed one billion units in 2014. Gartner Inc. Retrieved June 19, 2015.

Vinton, K. (2014, June 24). Mobile malware is on the rise, McAfee report reveals. Retrieved June 27, 2015. http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/

McAfee Security Advice Center. (n.d.). What is mobile malware? McAfee Inc. Retrieved June 15, 2015. http://home.mcafee.com/advicecenter/?id=ad_ms_wimm

Kaspersky Lab ZAO. (n.d.). Kaspersky security bulletin 2013. Retrieved July 13, 2015. https://report.kaspersky.com/

Garnaeva, M., Chebyshev, V., Makrushin, D., Unuchek, R., & Ivanov, A. (n.d.). Kaspersky security bulletin 2014. Overall statistics for 2014. Retrieved June 13, 2015. https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

Penning, Nicholas, Michael Hoffman, Jason Nikolai, and Yong Wang. Proc. of 2014 International conference on collaboration technologies and systems (CTS). N.p., 2014. Web. 30 June 2015.

Zhou, Yajin, and Xuxian Jiang. Proc. of 2012 IEEE symposium on security and privacy. N.p., 2012. Web. 11 July 2015.