Mobile Malware

Andrew Castillo

Randy Matos

William Chavez

Luisana Figuera

Pedro Cordon

Dr. Alexander Pons

2/28/2014

Ethical Hacking and Countermeasures

Group 10

I. Abstract:

Hidden to the general population a new threat is growing and could soon lead to the spread of a mass security crisis. Malware has found its way into our smartphones, no matter which operating system that phone is currently functioning on. It is a threat that has long been hypothesized but today this threat is real and is capable of causing more harm than previously imagined. In a recent study from "Juniper Research has found that 80% of smartphones remain unprotected from Malware attacks. [1]" Which is a truly horrific statistic. With the closing threat of Malware infiltration in smart phones, companies have started offering their services to keep smart phone users safe but many users remain completely unaware.

In this report the topics of past, present, and future advances in malware in mobile devices, along with a set of statistics will be used to demonstrate the ever growing threat. Malware, for those who do not know, is "software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. [2]" The general concept of "Mobile Malware", it isn't restricted to just smartphones. Due to the nature of malware being operating system dependent it leaves tablets and other handheld devices open to become infected. "Mobile Malware" is a new evil and those who remain unaware will be its victims.

II. History of Malware

The beginnings of Malware can be traced as far back as 1949 when John von Nuemann wrote an article on his "Theory of self-reproducing automata." This article was based on a lecture he gave earlier that year in the University of Illinois titled: "Theory and Organization of Complicated Automata." In his article we can see the concepts and beginnings of what Malware would become. Around 1962, some researchers from Bell Telephone Labs created a game that destroys software programs, although it wasn't used for malicious purposes, it was still potentially harmful to a computer. However, it wasn't until 1971 when the first true, self replicating malware was created at BBN Technologies by Bob Thomas. It was called "The Creeper." It was an experimental, self-replicating program to infect DEC PDP-10 computers running the TENEX OS. Using ARPANET, it was able to spread and once it infected your system, the message "I'm the creeper, catch me if you can!" would be displayed. They later had to create a program called "The Reaper" to delete The Creeper. But it wasn't until 1982 when Richard Skrenta became responsible for the first large-scale virus outbreak in history. He wrote the program named "Elk Cloner" for the Apple II system, which was the predominant PC at the time, and after the 50th boot, it would display a poem that he wrote. The year after, 1983, Frederick Cohen coined the term 'virus' to describe a self-replicating computer program. This term was a suggestion by his teacher Leonard Adleman because you could describe the operation of a "virus" as an "infection." We can see that most of these viruses or malware were created as practical jokes, things that would scare the average user into thinking they may lose their information or worse, their computer. Richard Skrenta was actually infamous for this with his friends; before creating the Elk Cloner, he would scare them by making weird messages come up whenever they used a floppy drive he lent them. But as more vital information began to get stored on personal computers, people realized these viruses could be used for malicious purposes. Trojans and worms that can steal information or monitor what you type began appearing as early as 2001. However, the first well known Trojan was the Zues Trojan, which was created around 2007. It became well known for targeting Windows-based PCs to steal banking information using key logging and it was able to compromise over 74,000 accounts on different websites. Now, this may have been a threat to your PC, but at the time most people wouldn't have even thought that their mobile phones were in danger. Wrong. As early as 2005 the first mobile phone virus, named Caribe, was created to infect the Symbian mobile OS. Using Bluetooth communication it was able to spread and infect other mobile phones and would display the message "Caribe" whenever the phone was turned on. In 2009 the first ever iPhone worm was created. Sporting the name "Ikee," it was able to infect jailbroken iPhones that had SSH installed and were using the default root password. This worm would change the wallpaper of your lockscreen to a picture of Rick Astley with the message: "ikee is never going to give you up." Yea, you just got Rick Rolled. As of 2011, it's reported that as much as 73,000 malware strains are written daily. Considering that mobile smart phones have slowly been replacing our PCs to do our daily tasks, we are more at risk now that these malwares are being more freely written for mobile phones. Just ask history what happened with PCs: It may have started as a practical joke, but soon it was used for malicious purposes. History will in fact repeat itself with smart

phones and we need to be ready to increase our mobile security.

III. Technical Examples of Mobile Malware

Malware that exists for mobile devices differs depending on the platform it's used for. The examples of malware that will be presented in this section are related towards cellular phones and tablets and have notoriety within the mobile community.

A famous example of an Android Trojan is Backdoor.AndroidOS.Obad.a. It is a multi-functional Trojan that enables remote connection and allows the user access to install programs to the phone for further infects the device. The Trojan spawned from vulnerability in the DEX2JAR software. DEX2JAR is a program that is used to convert an APK file into a JAR format, which is an executable java file format. Also an vulnerability in the Android operating system was introduced. The virus modifies the xml file (AndroidManifest.xml) to bypass Google standards and allows exploitation on the device. There isn't a user interface for the Backdoor.AndroidOS.Obad.a Trojan, and the program continues to work in the background processes of this phone.

Ikee, was the first worm that was known for iOS devices. The worm replaces the wallpaper with a photograph of the singer Rick Astley. It was done through ssh protocols that were made available by the process of jailbreaking an iOS device. Jailbreaking is the process of hacking into the iOS operating system and removing the restrictions applied by Apple. Apple's iOS operating system has seen its share of Trojan Horses through the App Store, which is closely monitored through by moderators. An example of the attack is a Russian application that pulled the user's contact book information and uploaded the contacts to a server. This app has been removed through the App Store after being closely monitored with Kaspersky anti-virus. Several instances have occurred in which users with jailbroken iPhones have had private data stolen from their phone. The name of the worm is iPhone/Privacy.A. The tool scans the Wi-Fi network and searches for jailbroken iPhones. After finding the phone the tool copies all data including SMS messages, videos, email and etc. The program is run on the background while the user continues to use their phone.

Available to Blackberry and now Android users, a Malware bot priced at $4000 can be used for the social engineering of electronic bank notifications and their users. Some of the features that come included with the bot are sending text messages; starting and stopping phone calls, getting a text messaging and call list, and recording voice.

Для пользователя доступны следующие команды:

Команда в админке	СМС команда	Действие
start sms	sms start	Включить переадресацию СМС
stop sms	sms stop	Выключить переадресацию СМС
start call	call start	Включить переадресацию звонков
stop call	call stop	Выключить переадресацию звонков
	change num +XXXXXXXXXX	Изменить управляющий номер
get sms	sms list	Получить список всех СМС
get call	call list	Получить список всех звонков
start rec	start record	Включить запись звука с микрофона
stop rec	stop record	Выключить запись звука с микрофона
send sms	sendSMS +XXXXXXXXXX:text	Отправить СМС на произвольный номер
start call to #	call start +XXXXXXXXXX	Включить переадресацию звонков на произвольный номер
contact list	contact list	Получить список контактов с устройства

Fig X. Command options that are sent to the victim's device

The Man-in-the-browser is a Trojan that infects a web browser by finding vulnerabilities within a web browser's security. A child of this type of malware is the Man-in-the-mobile (MitMo) Trojan that does the same but through mobile devices and handle's imitates two-step verification.

IV. Trends in Mobile Malware – Statistics

During the last years the mobile device world has become one of the principal targets for cybercriminals. According to IDC (International Data Corporation), during the first quarter of 2012, the Google operating system (Android) recorded a year over year rise of 145% in market share and sales, becoming the most attacked operating system due to its market share and open source architecture.

In 2013, nothing has significantly changed in terms of the mobile operating systems that are being targeted by malware, Android is still target number one and other OS get anywhere closer. At the start of 2013, McAfee Labs researchers counted 36,699 mobile malware samples, where the 97% of those samples were designed to attack Google Android; by the end of this year the mobile malware

samples reached 148,778 according to the Kaspersky Security Bulletin for 2013.

The reasons for this are Android's leading market position, based on the incidence of third party app stores and its open source architecture, which make it easy to use for everyone: app developers and malware authors as well. Therefore this trend is not expected to experience any change in further years. On the next graphs it is possible to see this trend and how it has changed over the past three years.

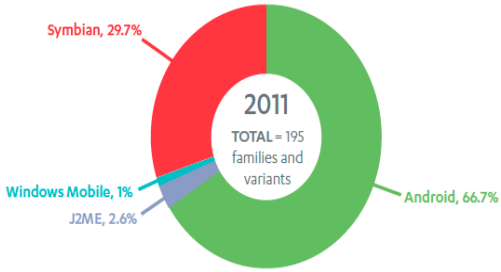


Fig A. Mobile Malware trend by OS (2011)[1]

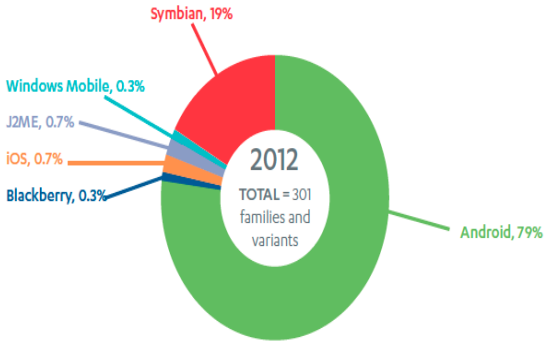
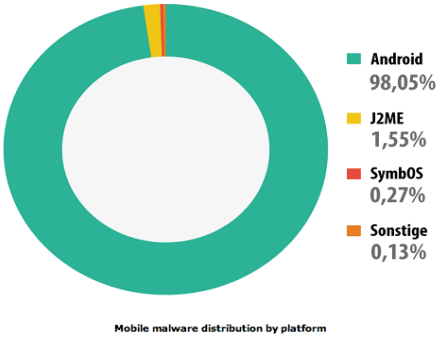


Fig B. Mobile Malware trend by OS (2012)[1]



Mobile Malware trend by OS (2013)[4]

The most critical factor that comes along with the mobile malware development has been the growing use of mobile devices as a form of secondary authentication for user credentials or online transactions. The most common manifestation of this is the mobile transaction authentication number (mtan), which is the authentication used by some banks during online banking transactions. Malware developers are currently able to avoid this extra level of protection by creating a mobile application that catches the SMS messages used to validate these transactions, one example of it is the popular mobile banking Trojan. On the next graph it is shown the malware distribution by behavior type.

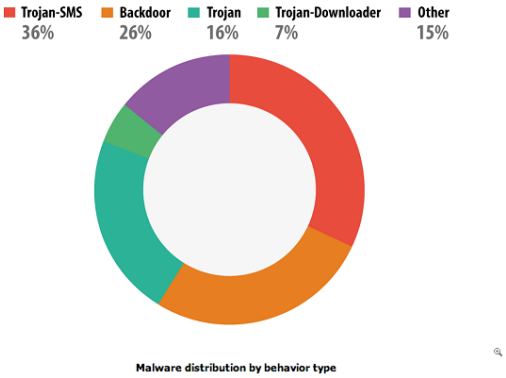


Fig C. Malware distribution by behavior type [4]

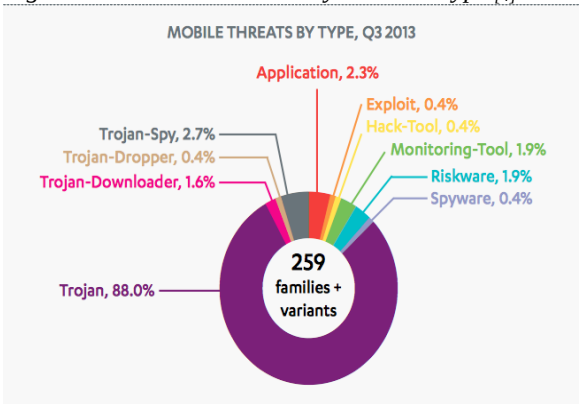


Fig D. Malware distribution by behavior type [2]

Finally, according to Juniper Networks the Mobile malware is becoming "an increasingly profit-driven business". Mobile vulnerabilities are no longer just a playground for cybercriminals, but have become a common practice to accomplish the new main purpose, which is the financial profit. The following graph shows the comparison between discovered threats that are profit-motivated versus non-profit-motivated ones.

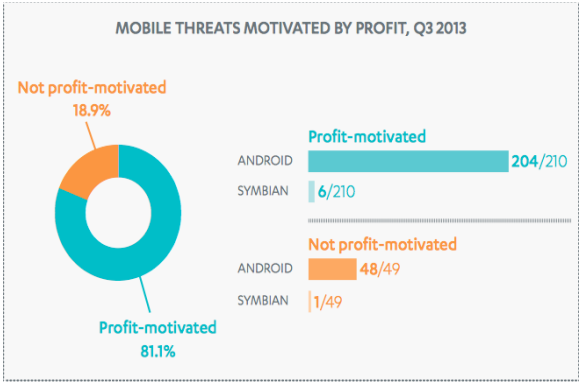


Fig E. Mobile Threats profit-motivated versus non-profit-motivated [2]

V. Future Examples of malware and research

a. Android: One Root To Own Them All

This is a vulnerability showcasing the technical details of Android security bug 8219321, disclosed to Google in February 2013. The vulnerability involves discrepancies in how Android applications are cryptographically verified & installed. It allows for APK code modification without breaking the cryptographic signature. Therefore, that in turn is a simple step away from system access & control. The vulnerability affects a wide number of Android devices, across generations & architectures, with little to no modifications of the exploit.

b. Android SpyPhone Service

The Android SpyPhone service can be injected into any Android application. Phones can be tracked and operated from a Web based command and control server. The application can be used to track the phone's location, intercept phone calls and SMS messages, extract e-mail and contact lists, and activate the camera and microphone without being detected.

c. Compromised CDMA Femtocell

A Femtocell is a low-power cellular base station given or sold to subscribers by mobile network operators. It works just like a small cell tower, using a home Internet connection to interface with the provider network. When in range, a mobile phone will connect to a femtocell as if it were a standard cell tower and send all its traffic through it without any indication to the user.

The state-of-the-art authentication protecting cell phone networks can be an imposing target. However, with the rising popularity of femtocells there is more than one way to attack a cellular network. Inside, they run Linux, and they can be hacked.

A femtocell can be used for traffic interception of voice/SMS/data, active network attacks, and can even be able to clone a mobile device without physical access..

d. iOS Device Malicious Chargers

Despite the plethora of defense mechanisms in iOS, it is possible to inject arbitrary software into current-generation Apple devices running the latest operating system (OS) software. All users are affected, because it requires neither a jailbroken device nor user interaction.

An iOS device can be compromised within one minute of being plugged into a malicious charger. USB capabilities can be leveraged to bypass these defense mechanisms. To ensure persistence of the resulting infection, an attacker can hide their software in the same way Apple hides its own built-in applications.

To demonstrate practical application of these vulnerabilities, a proof of concept malicious charger was built, called Mactans, using a BeagleBoard. This hardware illustrates the ease with which innocent-looking, malicious USB chargers can be constructed. While Mactans was built with limited amount of time and a small budget, it is mind bottling what more motivated, well-funded adversaries could accomplish.

VI. Conclusion

With the threat of “Mobile Malware” looming in the air, the desire to give the general public fair warning has never been greater. This paper was intended to provided that knowledge the general public needs and will reinforce the topic to those who were already aware.

The history of malware gave you a look into the not so distant past. The discussion of technical examples of malware was intended to show you how

rapidly the threat is developing along with the statistics of malware's current expansion, and the future examples of malware and research showed you concepts that were unimaginable to the common electronic consumer.

The majority of malware was originally designed to be a practical joke, but as we can see from the ever growing desire for malicious intent, the evolution of malware has followed suite. We can only hope that the growing need for security can be met.

VII. Reference

[1]http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/

[2]ESET Latin America's Lab. "Trends for 2014." 2013. 2014 <http://go.eset.com/us/resources/white-papers/Trends_for_2013_preview.pdf>.

[3]F-Secure. "Mobile Threat Report." 2013. 2014 <http://www.fsecure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf>.

[4]McAFee. Mobile Malware Growth Continuing in 2013. 2013. 2014 <http://www.mcafee.com/us/security-awareness/articles/mobile-malware-growth-continuing-2013.aspx>.

[5]SECURELIST. Kaspersky Security Bulletin 2013. Overall statistics for 2013. 2013. 2014 <http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013#04>.