2014

Mobile Device Vulnerabilities & Securities

Luke Rondeau
lrondeau2014@gmail.com

Mobile Device Vulnerabilities & Securities

Abstract
An investigation on current mobile vulnerabilities and research into security. Also, a proof of concept to show the ease of injecting an Android phone with a virus.

Degree Type
Open Access Senior Honors Thesis

Department
Technology Studies

First Advisor
Duane Hopkins

Second Advisor
James Banfield

Keywords
mobile malware, Android vulnerability, Zitmo, Android, Galaxy S2, malware injection

Subject Categories
Digital Communications and Networking | Information Security

MOBILE DEVICE VULNERABILITIES & SECURITIES

By

Luke P. Rondeau

A Senior Thesis Submitted to the

Eastern Michigan University

Honors College

In Partial Fulfillment of the Requirements for Graduation

with Honors in Information Assurance, College of Technology

Approved at Ypsilanti, Michigan, on this date: April 7, 2014

Table of Contents

Table of Figures

Introduction

Several years ago, it was only a dream to have a device that could go into your pocket and connect you to any person in the world. Several years ago it was only a dream that a 1TB hard drive could fit into the palm of your hand. Gordon Moore, a director of R&D for Fairchild Semiconductors, hypothesized that the number of components per chip would double every year in 1965. In 1975 he revised the rate to doubling every two years. This is where the term "Moore's Law" comes into play. Moore's law states that the number of transistors on an integrated circuit doubles about every two years. This means that a computer today is two times more powerful than a computer two years ago. So far this has held true and we are seeing computers complete operations we wouldn't have dreamed of in the past.

However with the creation of all the current technology we have including cell phones and laptop computers, there has also arisen a new type of criminal. This type of criminal is known as a cracker, hacker, or cyber criminal. With the increase of these types of criminals, instead of focusing on the traditional crimes, bank robbing, ATM theft, etc., computer devices have been subjected to onslaughts of attacks from these criminals. Now that mobile devices run the same processes and applications as a laptop computer, this has caused some new issues to arise that many people do not think about regarding the security of their mobile computers, leaving an opening that cyber criminals can exploit. With individuals upgrading to smartphones due to the fact that they make things not only more convenient, but also enhance productivity and connectivity for business people around the world, this is an important and serious security issues for all users, especially those using smartphones that are not secure.

The purpose of this research is to bring awareness on how cell phones work, expose the vulnerabilities of mobile devices, and to show the level of difficulty and probability that a particular cell phone can be infected with a malicious program. We conducted an investigation to show how easy it is to inject an Android mobile phone, the Galaxy S2, and infect it with a known banking malware called Zitmo. The reason for a banking malware instead of something else is the fact that banking malware can ruin someone's, life both monetarily and credit score, and lead a person into bankruptcy and is a smaller area of theft known as identity theft. Because smartphones are so ubiquitous and integral to our society today, it is imperative that technical research, like what is currently being investigated by professionals, reaches the hands of the public. Research showing a side-by-side comparison of different cell phone operating systems and their probability of getting infected with malicious programs, will allow users to make an informed purchase, raise public awareness that smartphones, when used incorrectly, can be dangerous, and force mobile phone operating system manufacturers to take an invested look into making their products safer. To understand the risks that mobile devices are exposed to, it is important to understand some basic concepts of malware and the people who create, distribute, and exploit them. In the next section we will go over some different terminology that is commonly used to describe computer and mobile device security and vulnerabilities.

What are the differences between a Hacker and Cracker?

To understand malware and cyber crime, a researcher must understand the people who do the crimes. Unfortunately the media, Hollywood, and novice to advanced technicians have not used the correct term for crackers and often refer to these types of cyber criminals as hackers even though there is a large difference between the two.

A paper written by Brian Harvy from the University of California, Berkeley, described a hacker as "someone who lives and breaths computers, who knows all about computers, who can get a computer to do anything." (Harvey, 1985) He then goes on to remark that to be a hacker, you have to use computers as a hobby, not a profession. (Harvey, 1985) Hackers cannot be professional thieves, which is what you are considered when you start to steal information from a computer or device.

Unfortunately calling cyber criminals a "hacker" is not the correct terminology to identify them. The correct term for a cyber criminal is a "cracker" or "cyber criminal". According to an article written by Margaret Rouse, most hackers deplore crackers, or those who break into computers. She reports that a cracker is "someone who breaks into someone else's computer system, often on a network, bypasses passwords or licenses in computer programs, or in other ways intentionally breaches computer security." (Rouse, 2007) Cybercrime, according to Dictionary.com, is "criminal activity or a crime that involves the Internet, a computer system, or computer technology". ("Cybercrime" n.d.) A cyber criminal, then, is someone who conducts a cybercrime and is often used when describing someone who conducts cybercrime. Cybercrime not only falls into someone cracking a network or computer and stealing data, but it also falls into the creation of malware, and more specifically, viruses.

What is Malware?

Malware is the general description for all items that negatively affect a computer or network system. The Massachusetts Institute of Technology (MIT) discusses on their website about what malware is and goes into detail about it, saying that;

> Malware is a term for any software that gets installed on your machine and performs unwanted tasks, often for some third party's benefit. Malware programs can range from being simple annoyances (pop-up advertising) to causing serious computer invasion and damage (e.g., stealing passwords and data or infecting other machines on the network.)" (Information Services & Technology, n.d.)

In the malware category, there are two other types of software that can cause either an annoyance to the user, or steal information. These programs are known as adware and spyware. Adware, according to MIT, is software that is supported by a program or company to show advertisements when you're online. Spyware is software that gathers information from your computer and sends it to others who would want this information. (Information Services & Technology, n.d.) This includes such things as an IP address, computer information like OS or computer model, etc.

Malware is a general term for different programs as discussed previously, but a more specific program family falls under the general categorization of malware and they are known as viruses.

What is a Virus?

According to Collins English dictionary, a virus is "an unauthorized program that inserts itself into a computer system and then propagates itself to other computers via networks or disks; when activated it interferes with the operation of the computer." ("Virus" n.d.) A virus is a specific term for a program that is installed on a computer and either does damage to the infected system or steals information right out of the hard drive and random access memory (RAM).

Matt Smith, a freelance writer out of Oregon, created an article on the website MakeUseOf.com about nine types of computer viruses to watch out for and what they do and is written so that anyone can understand it and is a good base for research to start on.

The first one researchers in this field should take a look in Mr. Smith's list is more directed to mobile devices that use a built in Internet browser like Internet Explorer, Chrome, Safari, etc. These viruses are called browser hijackers because they, in essence, hijack your browser and cause it to redirect you to a website, which can then install new viruses.

Another virus that is mentioned is the multipartite virus. This virus is a little more flexible than other viruses as it will run differently depending of the operating system that is installed on the device. Another feature that viruses like this can have is that it can scan a system for files that the malware engineer has an interest in, such as a file titled "password.txt".

In addition to a multipartite virus, there are the polymorphic viruses. When you break apart the word polymorphic, poly means many, and morphic indicates shape, form, or structure. ("Morphic" n.d.) Polymorphic viruses are viruses that can change, adept, and

can be customized for each infection if done correctly. This causes a massive issue for anti-viral and anti-malware programs, as you are unable to keep up with the changing virus. Ant-viral and anti-malware programs are programs that are installed on a computer or device that regularly scan the device for known malware and either alert the user or remove the infected file. Examples of anti-viral and anti-malware programs are AVG and Norton.

Finally according to Mr. Smith's list, phones can be exposed to web scripting viruses. Most phones access sites like YouTube.com, reddit.com, or Facebook.com, which utilize video players and videos posted on their websites. What this virus does is exploit the video code and will make it possible to download a virus to a computer when you go to play a video.

With an understanding of malware and viruses, researchers need to look into the history of cell phones and mobile devices to understand what these devices are and where they came from and why they are a good target for attack.

History of Cell Phones

Cell phones are the foundation for what smartphones were built upon. Because of this, knowing about how mobile phones work is extremely important to understand the vulnerabilities of smartphones. Robert Keith, an alumni from the University of Florida created a simple to read website discussing the general theory behind cell phones and their history, making mention to the specific years that marked large changes in the development of the phones. According to Mr. Keith the history of cell phones can be dated as far back as 1843, when Michael Faraday researched his hypothesis about if space can conduct electricity or not. It was not until 1865 when Dr. Mahlon Loomis, a Virginia scientist, developed a way to communicate through the atmosphere. He did this by flying two kites that were attached by copper screens and wires and grounded to two separate mountains about 18 miles away. The U.S. Congress gave him a grant for $50,000, for his research. (Keith, 2004)

It wasn't until 1921 when mobile phones and radios hit a milestone. That year the Detroit MI police installed mobile radios in their police cars. However, as we would see throughout this period until around the late 1950's into the 1960's, the radios were inconsistent and often transmissions were full of static, making it difficult to get messages sent. In 1934 the U.S. Congress established the Federal Communications Commission (FCC). Its primary responsibility was to handle all of the requests for frequencies and to organize rules and regulations pertaining to radio telecommunication. In 1945 the first mobile-radio telephone service was established. This service used six different channels that in total went up to 150 MHz's. The FCC approved this, but

because of the amount of interference, the system barely worked. During this time the majority of radio users were still police and some wealthy individuals. (Keith, 2004)

In 1949 the FCC finally authorized use of widespread separate radio channels to carriers who wished to use these radio channels. These were called Radio Common Carriers (RCC) and are considered the first link between mobile phones and the telephone. RCC's were designed more for money and to see a profit other than for the general public. It wasn't until 1964 when RCC's were considered legitimate competitors against landline phone companies. 1964 also saw the development and implementation of a new operating system that used a single channel at 150MHz. Five years later, in 1969, the frequency was bumped up to 450 MHz and these became the standard frequency in the U.S. (Keith, 2004)

In 1971, AT&T finally proposed their idea for mobile phones that turned into the modern-day system we use. They proposed to the FCC the division of cities into "cells" and included more detailed information about the framework including frequencies and how signals would get relayed. They were the first company to recommend this to the FCC. In 1973, Dr. Martin Cooper made the first call on a portable mobile phone. Dr. Cooper was working for Motorola and he took his invention, the Motorola Dyna-Tac, to New York City NY, and displayed it to the public. From that point to about 1988 cell phones saw an explosion of usage and technology, ranging from experiments conducted by Bell Telephone Company and AT&T in Chicago, IL in 1977, and the FCC's acknowledgement that they would have put the phone companies approximately seven years behind schedule if they had not ruled against Western Electric in 1974 during a law suite. Cell phones, or more commonly suitably known as "dumb phones" as they do have

all the "smart" features that smart phones have, increased in usage and number of units being sold to customers until the invention and mass usage of the smart phone. This is where the true vulnerability comes into play, as smart phones are nothing more than tiny computers.

History of Smartphones

On January 24 2012, Charles Arthur, an author with the Guardian published an article about the timeline of smartphones, including the introduction of the iPhone, Android, and Windows phones. According to this article, it started with the introduction of the iPhone on January 2007. The timeline ends January 2012, when the co-CEO and co-chairman of Research In Motion (RIM, better known as BlackBerry) resigned. (Arthur, 2012)

According to Mr. Arthur, once the iPhone took off, Microsoft was right behind them with their phone, the Windows Mobile Phone. Mr. Arthur reported that on April 2007, a technology research company named Gartner reported that within the first three months of the Windows mobile phone, Microsoft's attempt at a smart phone following the iPhone, had 18% of the share in the smartphone marketplace, which came to around 17 million handsets. Towards the end of 2007, Google stepped into the picture with their announcement of open source mobile OS called Android. When asked if Google would create a phone for their OS, Google's head of Android development, Andy Rubin, reported that there would be thousands of different phones with the Android software. This statement is true today because of the fact that the Android mobile OS platform is open source, or free to the public with no costs, and available to the public with little

difficulty through distribution websites, which is a contrast with Apple iOS which is secretive and locked down to many end users. (Arthur, 2012)

About a year later, Apple announced that it had sold 4.7 million iPhones. This was about 13% of the market share at that time. In comparison Research in Motion (RIM or better known as BlackBerry) had about 15%. One month later in November 2008, the first Android phone was released. Titled the G1, Mr. Arthur reported that it only had a slide-out keyboard and limited touchscreen. A month after that in December, Microsoft gave up on the Windows Mobile OS and ends the project as it couldn't keep up with Apple and Android. They then re-invest their time and energy into the Windows Phone OS that we see in some phones currently in 2013. (Arthur, 2012)

2010 was a big year for smartphones just like 2007, according to Mr. Arthur. In January 2010 Apple officially announced the iPad, which was revolutionary at the time and could be considered a smart phone as versions of the iPad use 3G and 4G data networks like cell phones. The next month Android followed suit with their first Android phones that had full touchscreen capabilities similar to the iPhone. However a month after Android released their touchscreen phones, Apple felt their technology was being copied without their consent, which started a very long legal battle that still continues into 2013 and 2014. (Arthur, 2012) Steve Jobs, then-CEO of Apple, met with Google CEO Eric Schmidt and threatened him about the similarities between the Android phone and the iPhone. That same month Apple takes a similar matter to the courts and sues Taiwan's HTC for patent violations. (Arthur, 2012)

According to Mr. Arthur, 2011 saw a flurry of activity, just like 2010, starting with Gartner researchers and International Data Corporation (IDC) announcing that in the

last quarter of 2010, smartphones outsold PC's 100 million to 93 million. February 2011 saw the introduction of the Windows Phone OS into Nokia handsets. April and June saw a number of legal issues come up. With Apple becoming the largest smartphone vendor (18.6 million iPhones to 17.5 million Samsung phones), Apple sues Samsung over the Galaxy Tab tablet, following that up with several other cases around the world for patent infringements. In June of 2011, Microsoft starts requiring royalties, which Samsung and HTC to comply with. In the following months, numbers of tablets and smartphones keep increasing with Samsung and Android taking the lead in number of units and OS's sold. (Arthur, 2012)

Once we understand the history behind cell phones and smart phones, we need to take a look at how they actually function, as most exploits will use their functions to send stolen data back to the original malware engineer.

How Do Mobile Cell Phones Work?

It is important to note that cell phones are nothing more than complex radios. Cell phones operate on the basic principle that your voice and internet requests are sent via a antenna to a cell tower, who then processes the request and either redirects it to another tower to be directed to the destination, or sent into the Internet to retrieve the data that is being requested.

Mobile phones operate on the same principles that current very high frequency (VHF) and high frequency (HF) radios operates on, but are more complex than their "push-to-talk" siblings. A push-to-talk radio is a device that has a "transmit" button, normally located on the side, and the sender must engage this button to have the radio go from receive mode to transmit mode. The operator is then allowed to speak, which will be broadcast from the radio. To have a radio communicate with another radio the operator must be on a particular frequency, normally notated by MHz as in 50MHz. Once this connection is established, the operator is able to transmit over this frequency normally utilizing a radio antenna or base station and repeater.

Radios normally operate using a simplex or duplex method of their frequency assignment. Simplex is a "simple" way of assigning frequencies. Simplex devices normally have one radio frequency assigned for both transmission and receiving. Some examples of simplex radios are family hand-to-hand radios and garage openers. A duplex system is what cell phones and radio repeaters use. Radio repeaters are devices that take incoming radio waves and repeats them out, normally with more power than the radio that initially sent out the transmission. They are normally able to have both transmitting and receiving features, which means they are able to hear and talk at the same time. For

example, VHF radio repeaters are able to take an incoming radio transmission and repeat it right back out via a different frequency without having to wait for the sender to stop transmitting. Cell phones operate in a similar way, as demonstrated by a situation in which two people get into an argument over the phone. Both parties are able to hear and talk to each other at the same time; even their phones are sending and receiving signals at the same time, which is not possible on a simplex system.

The website HowStuffWorks.com, a website operated under the Discovery channel, describes in detail how cell phones operate from the early ages of analog transmissions to 3G data digitized transmissions. Cell phones utilize a similar method but each large urban area is divided into a "cell", normally of a hexagon shape. These areas have one base station per cell and a Mobile Telephone Switching Office (MTSO) controls each large urban area, normally comprised of several cells. Each cell tower has a unique system identification code, which identifies the carrier and either the cell phone or the tower. Once the codes are exchanged from cell phone to tower the phone is assigned a frequency where it can then contact anyone who is also in range of a cell phone tower and connected to the network.

3G and 4G cell phone data signals operate in the same way, however, their MHz's are in a much higher band. Also while pre 2G (or 2nd generation) phones use analog for sending and transmitting voice transmissions, 2G and beyond use advanced protocols that take your voice and digitize it into ones and zeros and sends them in packets similar to what you find while using your internet at home. This is where the danger of cell phone hacking comes into play.

Because you are now connected to the internet, you are not only exposed to the normal threat of viruses embedded in videos and "free" music downloads, but there are others who are looking to steal the data off your phone. The way that this can be done is through a virus installed on your device that stays hidden, or by stealing the device itself and getting into it using a variety of back-door exploits (errors in the code that crackers utilize to enter a system without the administrator or user knowing about, like a backdoor into a house or bank). There is a clear difference, however, between cell phones and smart phones. These differences also play an important role in their vulnerabilities.

Now that we understand how cell phones and mobile devices work, the history behind them, and some common terminology that malware researches use when studying malware and infections, we have to understand why we research these issues and statistics are a very strong way of showing if an issue is something to investigate further or not.

Current Statistics

Statistics are a strong piece of research when people go to talk about why computer security and mobile device security is important. It is something most Chief Information Officers (CIO's) will use when presenting their findings to management boards for funding or to raise awareness on a particular issue that the company is experiencing. To accurately analyze the statistics of mobile malware we have to establish a baseline comparison, and then investigate data leading up to the most resent statistical report.

Blue Coat Systems 2013 Mobile Malware Report

To establish a baseline to compare other security statistics to, Blue Coat Systems created a report towards the end of 2012 showing the trends, how infection rates were increasing, and to offer projections for 2013 and what to prepare for. According to Blue Coat (2013, p. 3), the key points they found in 2012 were:

1. Mobile threats are still more for inconvenience as compared to viruses that infect desktop and laptop computing systems.
2. As it was when computers first started being infected via the web, the most common types of malware are spam, scam, and phishing attempts.
3. Currently pornography is showing to be a huge weakness for mobile users. If the user visits a porn site on your mobile device, the probability of infection goes up three times higher as if the user were on a computer.
4. While smaller than their desktop counterparts, malnets (networks of malware infected computers targeting other computers) are setting their sights on mobile users.

5. Finally it is important for businesses to extend security towards mobile devices, especially since the practice "Bring Your Own Device", or BYOD, is common in the workplace. (Blue Coat, 2013, p. 3)

To properly understand the risks with mobile malware you have to know how each user interacts with their device and how much time they spend on different utilities and services offered through the device. Blue Coats reported that users spend 72 minutes on average using their devices, which is the most vulnerable time for a user and their device. (Blue Coat, 2012, p. 6) Breaking down the 72 minutes, Blue Coat reported "more than 11 minutes with content related to computers/Internet. The remaining 60 minutes are spent looking at a variety of content, ranging from social networking and shopping to business/economy and entertainment." (Blue Coat, 2012, p. 6)

The reason for this is because of the types of malware that were being introduced into the system. For example: phishing e-mails, which are e-mails that seem legitimate, are received into a user's inbox and pose as something like PayPal account management. The e-mail may say something along the lines of the user's account was blocked for malicious activity or something as simple as "We are updating our systems and per policy 132.2A we must request all PayPal patrons to re-enter and confirm their enrollment in the PayPal service." This will direct the user to a link and the user will put in their information, which is then sent to the criminal who now has access to the user's PayPal or other accounts.

Blue Coat then showed the statistics of desktop versus mobile web usage. Regarding to social networking, 13.35% of requests were from mobile applications compared to 11.25% on desktop. For search engines and portals, only 8.47% were from

mobile devices in comparison with 19.26% from desktop. Audio and video clips were also higher than mobile with a comparison of 5.65% for desktops to 0.94% for mobile devices. However, news and media were higher with the mobile web use at 5.61% compared to 1.96% and recreation was also higher with 9% being mobile web usage compared to desktop usage of only 4.18%. (Blue Coat, 2012, p. 7)

It is often believed that the user is the weakest link in any security model. This is not because users are believed to be "dumb" or "stupid", but unfortunately user interaction and behavior often becomes a systems Achilles heel. (Blue Coat, 2012, p. 9) Blue Coat reported that the top threat categories for mobile users were, in order: Pornography, suspicious (spam, scam, phishing), entertainment, & unrated. There are other threats that are dangerous to mobile phones and desktops but these threats are more dangerous on a mobile computer than their desktop counterparts. (Blue Coat, 2012, p. 9) Looking deeper into those threat categories, Blue Coat showed that as far as percentage of requests from mobile devices to dangerous vector categories are concerned, 2.23% were pornography, 1.71% were spam, 1.52% were suspicious, and 1.34% were phishing. Also they showed that the unique site requests had spam as the leading malicious vector with 4.39% of all requests, pornography and proxy avoidance following behind with 3.8% and 1.2% respectively.

According to Blue Coats, out of all of the malware they blocked using their WebPulse system, 58% of all malware blocked was Android root exploits, or vulnerabilities in the systems basic programming. Another 40% was Android malware via malnets, and one percent was both unique Android malware URLs and unique

Android malicious applications. (Blue Coat, 2012, p. 13) This means that the target in the mobile malware front is Android systems.

As a baseline for the other two statistical analyses, the Blue Coat article shows that mobile malware was increasing during 2012 and into 2013. With this baseline, researchers are now able to compare reports that are published during 2013 and identify current trends that are on the rise, or trends that are currently beginning to disappear and better focus their efforts on areas that are considered more dangerous and vulnerable than other areas.

McAfee Threats Report: Second Quarter 2013

McAfee, best known for their anti-viral and anti-malware software, published a report regarding the second quarter statistics for 2013 regarding computer threats. These statistics involved the months of April through June which show a more accurate report of what we are currently experiencing and can also show us where malware is moving to when you compare the statistics to Blue Coat's report for the end of 2012. McAfee reported "Backdoor Trojans and banking malware were the most popular mobile threats this quarter. We counted more than 17,000 new Android samples during this period." (McAfee Labs, 2013, p. 3)

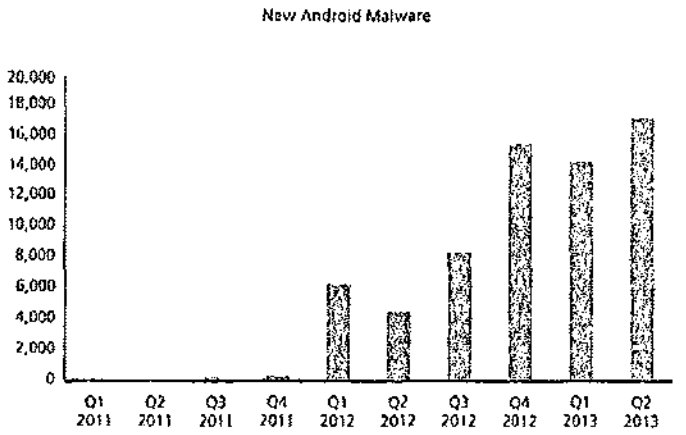

Figure 1: New Android Malware (McAfee Labs, 2013, p.6)

Further in their report they note that just in half of 2013, they had collected as many new mobile malware as they did in all of 2012, a comparison of around 35,000 by the end of 2012 to just above 30,000 in the middle of 2013.

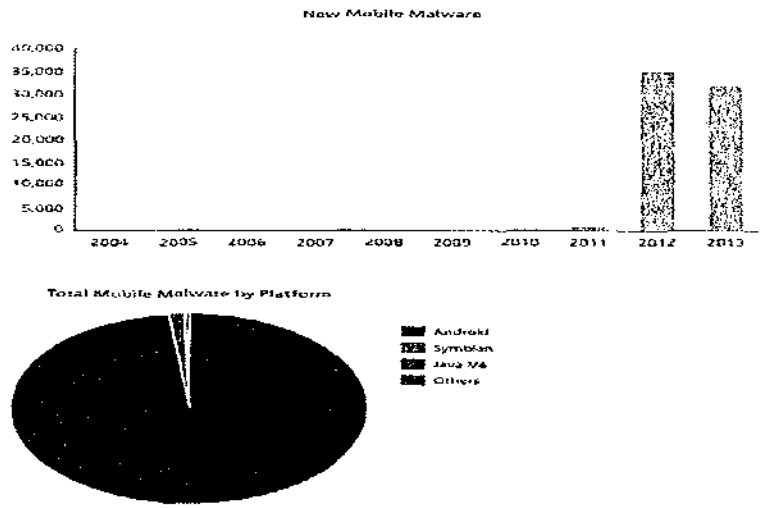

Figure 2: New Mobile Malware and Division of OS infection (McAfee Labs, 2013, p. 5)

As Blue Coat mentioned in their report, McAfee also reports that pornography is a major threat to mobile users. In particular McAfee talks about adult dating sites and a particular virus known as Android/Dcaifraud. This virus pretends to be an app for an

adult dating site and steals personal information from the phone. This virus, according to McAfee, was mostly found in Japan. McAfee then reported about two viruses noted in the second quarter, Android/NMPHost.A and Android/NMP.A. Android/NMPHost.A injected the phone with Android/NMP.A and once Android/NMP.A was injected into the phone it stole sensitive information and sent it back to the attacker's server.

McAfee reported that at the end of second quarter of 2013, they had over 147 million samples in their malware collection or what they referred to as their "zoo". (McAfee Labs, 2013, p. 7) Based on their data they pulled from July 2012 to June 2013, malware is on the rise with no period of decrease or staying the same. This data is alarming, especially since malware keeps rising and security with mobile devices not currently matching the amount of malware being published, especially for Android systems.

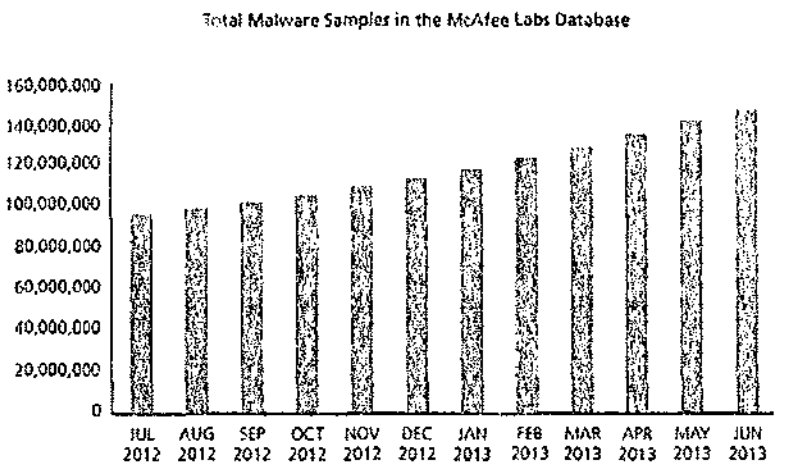

Figure 3: Total Malware Samples in McAfee Labs Database (McAfee Labs, 2013, p. 7)

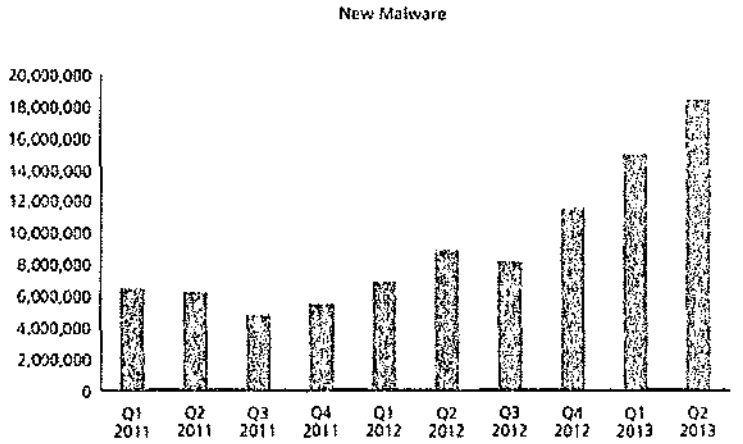

Figure 4: New Malware Detected by McAfee (McAfee Labs, 2013, p. 8)

While looking at malware in general, McAfee reported that even though it had shown a decline during quarter one, malware bounced back sharply with more than 1.2 million new samples. Shown are McAfee's data regarding new malware detected for each quarter and total malicious signed binaries, or code, for each month.

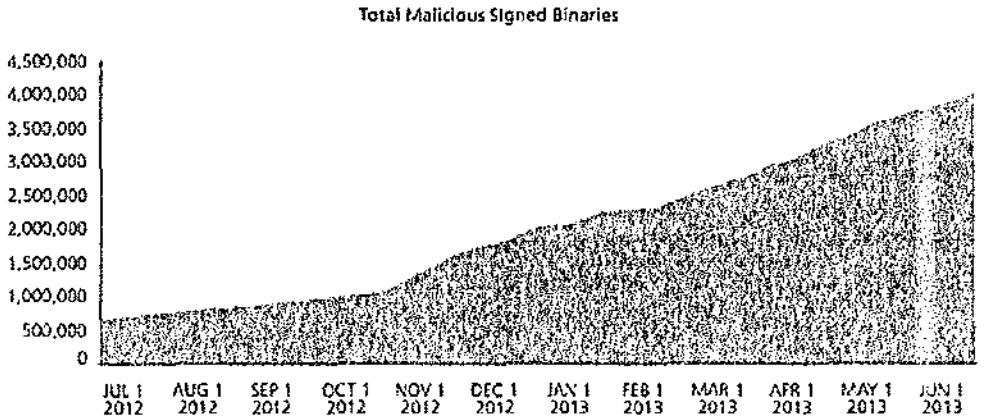

Figure 5: Total Malicious Signed Binaries (McAfee Labs, 2013, p. 11)

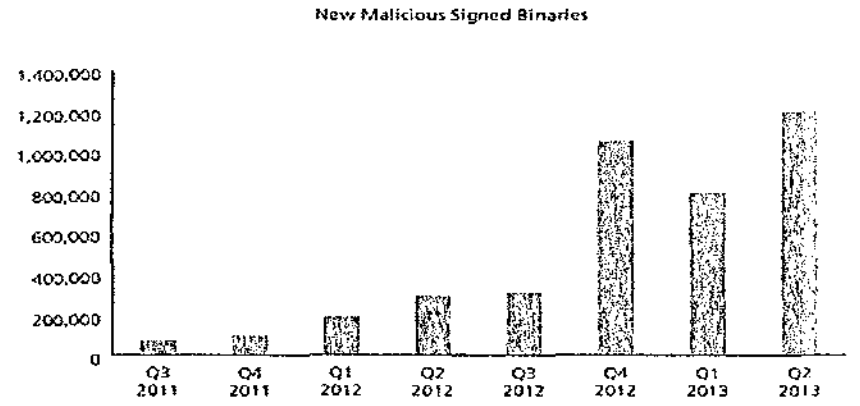

Figure 6: New Malicious Signed Binaries (McAfee Labs, 2013, p. 12)

As was mentioned by Blue Coat, suspicious malware URL's were on the rise as reported by McAfee. According to the graph, the number of URL's went down in the first quarter to just above 6,000,000 but climbed quickly to close to 11,000,000 by the end of the second quarter. (McAfee Labs, 2013, p. 17)

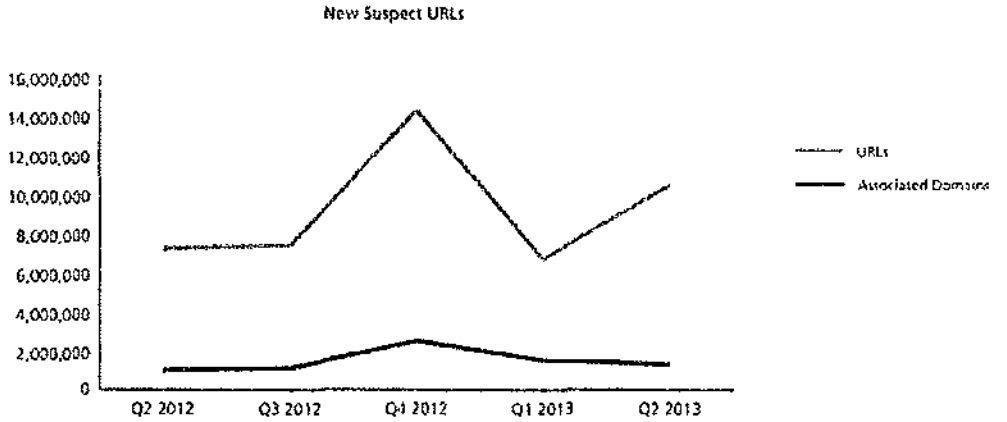

Figure 7: New Suspect URLs (McAfee Labs, 2013, p. 17)

Because phones are now commonly used to check e-mails on the fly, it is important to take note of the number of monthly spam messages as compared to legitimate e-mail messages a user may receive. McAfee saw a sharp increase in the number of spam messages from February 2013 to April, and then the number decreased

to June 2013. In April, the number of monthly spam messages peaked at over 2.0 trillion messages while at the same time, legitimate e-mails were only at a little over 0.5 trillion. By the end of June the number of spam messages had decreased to around 1.7 trillion but legitimate e-mails were at around 0.4 trillion.

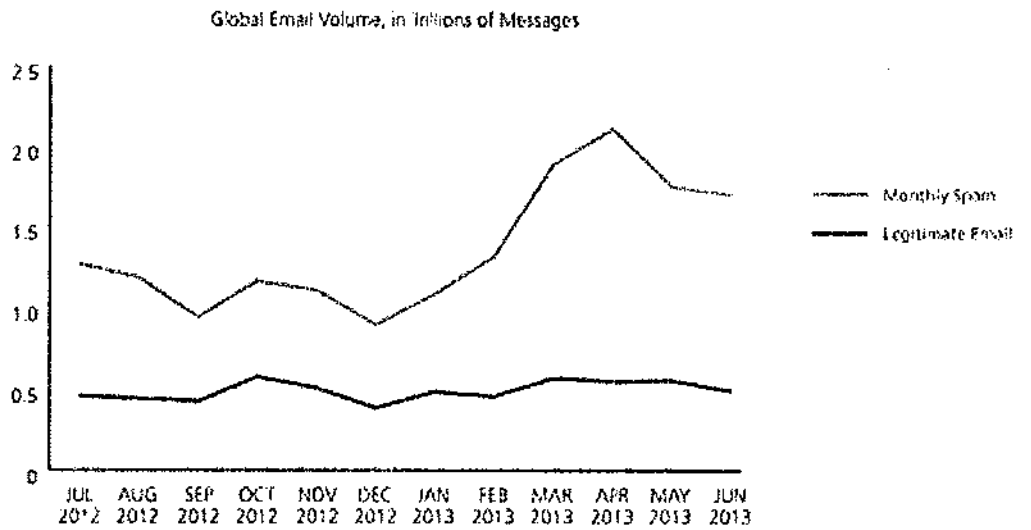

Figure 8: Global Email Volume, in Trillions of Messages (McAfee, 2013, p. 22)

When compared to McAfee and Blue Coat, it becomes increasingly clear that malware and viruses are increasing. However because the field of computers changes drastically, researchers must look at the most current research and statistics to better gauge current threat trends because a threat one quarter may no longer be one in the next. F-Secure's mobile threat report for July – September 2013 will provide the most accurate statistics currently.

F-Secure: Mobile Threat Report, July – September 2013

Because the fourth quarter is still in progress at the time of writing this research, the third quarter statistics of 2013 are the most accurate detailing the current situation regarding malware especially mobile malware. F-Secure published their third quarter

findings on mobile threats and show the current landscape for accurately projecting and identifying problem areas.

F-Secure reports that "Out of the 259 new threat families and new variants of existing families discovered in Q3 2013, 252 were Android threats while the other seven were Symbian. No malware has been yet to be recorded in 2013 on the other platforms (Blackberry, iOS, Windows Phone)." (F-Secure, 2013, p. 4) Figure 9 visually represents these statistics.

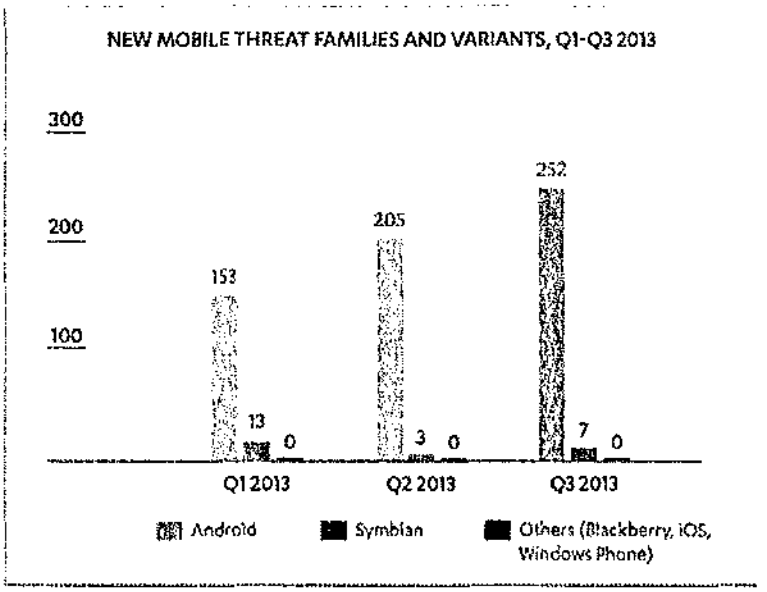

Figure 9: New Mobile Threat Families and Variants, Q1-Q3 2013 (F-Secure, 2013, p.5)

F-Secure touches on the subject of mobile banking security, which our focus for the proof of concept, Zitmo, is exactly related to.

> One of the critical factors driving mobile malware development has been the growing use of mobile devices as a security check, usually as a form of secondary or two-factor authentication for user credentials or online transactions. The most common manifestation of

> this is the mTAN (mobile Transaction Authentication Number) authentication used by during online banking transactions by some banks as an added extra level of security. Malware authors are currently able to circumvent this extra level of protection by creating a mobile program or application that explicitly intercepts the SMS messages used to validate these transactions - thus the birth of mobile Banking Trojans. (F-Secure, 2013, p. 7)

Now that we have these three statistical reports, we are able to accurately identify that the trend of mobile malware and malware in general, is on the rise. This is why researchers, like those from Kindsight, the National Yunlin University of Science and Technology, Louisiana State University, and the University of Michigan, have done research into mobile security and also computer security as a whole.

Current Research into Mobile Security and Vulnerabilities

Since this is still a new field of research, it is ongoing and always finds new vulnerabilities with ways to protect mobile devices and cell phones against possible intrusion. Another malware detection systems provider, Kindsight, has done research and reported on both Zeus, which is the desktop virus associated with Zitmo, and Zitmo itself. Moving away from the details of Zitmo and Zeus, one research paper that talked directly about mobile security and vulnerabilities was the result of a combination of several students and faculty from Taiwan and the United States. Their paper is a critical survey regarding security of mobile phones and mobile phone viruses. As the authors have done a lot of research regarding mobile security overall it is important for researchers to consider the information they have already found and noted in their report *Security Aspects of Mobile Phone Virus: A Critical Survey*

Security Aspects of Mobile Phone Virus: A Critical Survey

Emerald Group Publishing Limited published a paper written by four authors; three of who are from Taiwan and the other is from the United States of America. The authors from Taiwan are Dong-Her Shih and Hsiu-Sen Chiang from the National Yunlin University of Science and Technology and Ming-Hung Shih from the National Chiao Tung University. Binshan Lin is from the USA and was apart of Louisiana State University. The reason for this research is because it is important to understand how complex an issue mobile security and vulnerabilities are.

To properly introduce their topic and understand the immensity of the issue, they start the research paper "In 1986, there was only one known computer virus. Today, there are almost 60,000 viruses in existence and they have gone from being a nuisance to a

permanent menace." (Chiang, Lin, Shih, & Shih, 2008, p. 1) In a sense from 1986 to 2008 when this research was published, 59,999 viruses that were created and it's not just the sheer number of new viruses, but how deadly they have gotten when infecting a computer.

The researcher went into a discussion about the history of the virus and its first infection of mobile cell phones and then continues up until around the date of publication where the researchers talk about the first cross-platform attempted virus. According to the researchers, the first virus was found on May 30 2000 and was designated VBS.Timofonica. According to Symantec, the VBS.Timofonica virus is categorized as a worm malware. Worms, according to Cisco, are similar to viruses in the fact that they replicate copies of themselves and do the same kind of damage. However unlike viruses, worms are a stand alone application that does not require a host program or human.

Referencing back to Symantec VBS.Timofonica is also known as I-Worm.Timeofonica, VBS/Timofonica and VBS/Timo-A. They report that the last rapid release date was September 28 2010 and their threat assessment is good as they show it is ranked as "low" out in the wild only showing about 0-49 infections and it's containment and removal are easy. In short, Symantec has rated VBS.Timofonica as a risk level two. (Ewell, 2007)

The first reported transmission of a virus over a signal was the Cabir proof-of-concept mobile virus that was introduced in June 2004. A computer scientist created this particular virus and it used Bluetooth signals to send itself over the airwaves to other victims who thought they "received a security program and proceeded to infect themselves upon installation." (Chiang, Lin, Shih, & Shih, 2008, p. 2) In that same year

but a month later the first virus to infect Windows mobile operating systems was released.

In August of 2004, the Trojan virus was released that started to infect phones via a short message service (SMS) text. According to Chiang, Lin, Shih & Shih (2008) the virus was engineered by a company named Ojam. What that company had done was "engineered an anti-piracy Trojan virus in older versions of their mobile phone game Mosquito. This virus sent short message service (SMS) text messages to the company without the user's knowledge." (Chiang, Lin, Shih, & Shih, 2008, p. 2) The researchers reported that this was removed from future versions of the game, but may be found on the older versions floating around the free-software world.

A year later in September, a malware designated CARDTRP.A was released and tried to be the first cross-platform mobile worm. This worm included WUKILL.B that was a worm that tried to ruin the Windows operating system. According to the researchers this worm infected the memory cards of mobile phones and when the memory card was connected to a Windows computer, it tried to open a backdoor and distribute two more worms. The researchers report that historically this worm was not exactly successful but it did demonstrate that viruses and malware were evolving.

According to Robert Wang, software engineer at Symantec (2007), the full name of this virus is SymbOS.Cardtrp.A. Symantec classified this virus as a Trojan horse and affected EPOC systems. The initial rapid release version was dated September 22nd 2005 and it's last rapid release version was dated August 20 2008. Symantec classified this virus as a risk level one which is very low as its geographical distribution was low and its' containment and removal was rated as easy. (Wang, 2007)

According to Heather Shannon another member of the Symantec writing team (2007), the full name of the second worm that CARDTRP.A carried was called W32.Wullik.B@mm. Symantec classified this as a worm and it affected the Windows 2000, 95, 98, Me, NT, and XP operating systems. This worm is also known as Bloodhound.W32.VBWORM and W32/Wukill.worm [McAfee]. On Symantec's report of this worm they report that it is a "mass mailing worm that attempts to send itself to all the contacts in the Outlook address book." (Shannon, 2007) According to its' initial rapid release date of November 7th 2003, this worm was around well before the CARDTRP.A virus was created, meaning that the version of W32.Wullik.B@mm must have been through several rounds of revisions. Symantec rated this as a risk level two, which is low because its geographical distribution for the malware was rated low and it is easy to contain but it is moderately difficult to remove. (Shannon, 2007)

Something interesting that the researchers did in their paper was to tackle some mobile phone myths that many people believe. The reason understanding these myths is similar to the theory that the user is the Achilles Heel of any security framework. The first myth they tackled is the myth that "I did not run the executable file on my phone, so my phone is safe." The researchers had a point when they said that opening infected e-mails can infect your system, but two things they never covered were installation of new applications from "App stores" and the use of mobile devices to view videos on Facebook, Twitter, and YouTube. (Chiang, Lin, Shih, & Shih, 2008, p. 4)

Humans are drawn to the things that say "free" on them. This includes mobile device applications that are free and most, when downloaded from a trusted applications store like Google Play, the App Store, or Windows Marketplace, can be safe and

enjoyable. However when people install free apps from third party sites or apps that people "recommend" on Facebook, this can install viruses and other nasty malware that the user didn't realize was a trap. There are also vulnerabilities that can be exploited when someone plays a video off of Facebook or YouTube. These can cause malware to be installed onto the phone and then spread to either other victims or the original victim's main computer when they hook it up to sync between phone and computer.

The next myth that the researchers tackled was the myth that "The computer virus didn't infect the mobile phone, so my phone is safe." (Chiang, Lin, Shih, & Shih, 2008, p. 5)There are two major things wrong with this statement: How do you know that the virus didn't infect your phone and what anti-viral software do you have on your phone that allows you to scan it and verify that it is safe? A virus that attacked Droid mobile phones infected the phone and hid inside some random files that are normally not scanned during sync. The virus then attached to files being sent over the USB cable and infected the computer. The opposite is true and probable. Crackers understand that if you can infect the phone and the computer, that's double the amount of information, you are retrieving and that, in theory, is double the money you can sell out to those who want it on the black market.

The myth about having a firewall set up so your e-mail is safe is false. (Chiang, Lin, Shih, & Shih, 2008, p. 5) Firewalls only protect the devices that are on the protected side of it. Since most mobile phones are not on the protected side of a firewall this doesn't exactly apply unless the myth is referring to the firewalls in place at the e-mail server's location. Even then fake e-mails make it through all the time from "trusted"

sources that have been hacked and that voids the protection of the firewall because it's coming from a "trusted" source as far as the firewall's protocols are concerned.

The last three myths that the researchers looked into were the myth that if someone uses something other than a smartphone, often referred to as a dumb phone, they only browsed web pages and never downloaded something, and they only played games on their phone, means they are safe. (Chiang, Lin, Shih, & Shih, 2008, p. 5)The researchers responded to these myths in a very straightforward way that still applies to today's mobile phone technology. For the first myth they did admit that yes because dumb phones have such closed operating systems that the incidents of infection were diffused but it still happens. The only issue with dumb phones is the fact that everything is starting to move towards utilizing smartphones for day-to-day transactions like coupons at the store or digital key tokens for work place VPN's installed as an application on your phone.

The next myth regarding viewing webpages on your mobile device is very true: No matter how you view a webpage, there is always a risk that the URL is either a fake one or the site has been hacked and will run and install malware utilizing such things as JavaScript and the Microsoft VM ActiveX control vulnerability.

The final myth of playing only a game on a mobile phone so it's safe is completely false. Games installed on mobile devices, as the researchers noted in their paper, run code for the game but can run malicious code in the background, virtually going undetected because you are focused on the content of the game.

Understanding the myths that users believe to be truth will allow researchers to identify areas that infection and attacks can come from as this defines a particular area

that is left vulnerable. Ignorance by a user with their phone can be compared to someone leaving their purse on the seat of their car and just locking the door. It's a matter of a criminal wants that information and doesn't care if the door is locked or not as the windows are easy to break. With the knowledge of some common myths, research can focus on the malware used in the experimentation and any accompanying viruses that help in the infection.

Trojan Virus: Zeus

The first item that must be addressed is the malware known as Zeus. This is the primary malware associated with the Zitmo malware that is used for the laboratory proof of concept. In comparison to Zitmo, Zeus collects more information using methods like key logging, browser spying, information interception, etc. According to Kindsight (2010), they say that Zeus "attaches itself to your web browser, which enables it to monitor everything you do on the Internet, including your online banking and credit card transactions." (Kindsight, 2010)

Kindsight goes into detail about how Zeus interacted with the web browser, saying that it "records everything you type in, including user IDs, passwords, bank-account numbers, credit-card and PIN numbers and sends them back to the cyber-criminal's computer where the information is stored in a sophisticated database. (Kindsight, 2010). This, in combination with Zitmo's ability to send and receive SMS messages, full Internet access on the phone, and ability to intercept phone calls, makes the combination serious to mobile and computer users.

Trojan Virus: Zitmo

Zitmo, according to Kindsight, is the Android version of Zeus. This malware "works in conjunction with the Zeus banking Trojan to steal login information or money from your bank account." (Kindsight, 2011) They go into detail on how Zitmo accomplishes this, which utilizes "a number of interesting techniques including phishing, pretending to be a security application, intercepting SMS messages and sending authentication credentials to a remote server." (Kindsight, 2011) This means that if your computer is infected with the Zeus Trojan, which after visiting the Trusteer Rapport online site to register the Trojan application, and the Zitmo application on your mobile phone, a malware engineer has the ability to collect a wealth of information on your banking habits and all of your financial information, making identify theft even easier.

In most science disciplines, a researcher not only writes about other research in the field that they are studying, providing statistics that backs his or her claims, and also discusses major terms specific to his field, the research will also conduct experimentation or create a "proof of concept" as an original addition to the study of his field. To demonstrate how vulnerable phones are when not used properly, a proof of concept was planned and carried out using an Android mobile phone and the Zitmo virus described previously.

Proof of Concept and Malware Analysis

For the proof of concept and malware analysis, an Android OS was selected as the testing bed for infection. The reason for this is also a reason for the climb in malware usage and vulnerabilities. Android operating systems, due to its "open source" nature, makes it a very likely breeding ground for mobile malware. Because of how open the operating system is to end-users, malware engineers have the ability to really look inside the system, find all of the system vulnerabilities, and exploit them. The other reason the infection rate could be so high is because Android phones have a majority of the market, even though it seems Apple iPhones are more prevalent in society. Apple is also protective about their iOS system, meaning it is extremely hard to get ahold of for experimentation and malware engineers understand the "money" is in Android malware.

The objective of this proof of concept is to see how easy it is to infect an Android mobile device with the Zitmo virus.

Materials:

The materials used for this proof of concept were:

- 1 Galaxy S2 Sprint Android Phone
- Android 4.0.4 "Ice Cream Sandwich" PDA Flash file
- Celebrite Mobile Phone Imaging Machine
- Laptop Computer
- USB Connector Cables
- FTK Imager
- Process Monitor
- Super One Click rooting tool

- Logcat
- Camtasia
- Zitmo.apk file
- SDK toolkit including adb shell access.
- All documentation regarding rooting Android OS's, logcat, adb shell commands, and Zitmo documentation.

Safety Precautions:

Because we were dealing with a live virus, certain safety precautions were taken to ensure not only the safety of the data inside of the phone, but also the safety and security of hardware and network systems.

All programs were updated before initial download of the Zitmo.zip file from Contagio malware dump. Contagio is a site used to house samples of malware for analysis and investigations such as this one. The laptop, once all updates were applied and all necessary programs installed, was imaged onto another hard drive, ensuring that should the testing hard drive get infected, we could quickly remove it from the system and wipe it, without risking all data loss from previous investigations and data collected.

The phone was removed from the wireless system and not activated, which means it could not talk to the Sprint system. The phone's OS was also flashed, which means that a fresh unrooted version of Android Ice Cream Sandwich could be installed. Once the phone was flashed and removed from all networks, the phone was imaged using a Celebrite machine that allows for imaging phones in forensic investigations.

All data removed from the testing laptop was scanned with up-to-date anti-viral and anti-malware programs and the actual Zitmo APK file was not allowed to be moved onto any device other than the testing phone.

Proof of Concept

For the creation of the proof of concept, we obtained the required hardware and proceeded with the first option in mobile device infection: rooting the phone and installing third party application via injection from the computer to the phone via USB cable. This process required the use of SuperOneClick to exploit a known vulnerability in the phone, causing it to be in a rooted state. To root a phone means that you exploit a vulnerability, which allows the creation of a "super user" account. This account allows access to system files and processes that are normally hidden at the deeper level of the process tree.

The second part of the investigation in the forensics lab was to inject the phone with the malware APK file directly with an unrooted phone, but the option to download applications from third party sites checked. This process is very similar to the process above via injection of the malware using a USB cable and observing the interactions of the phone's systems and the malware, however the phone was not run through SuperOneClick and was not rooted.

Laboratory Malware Investigation

The overall goal of the research after the proof of concept experiment was complete, was to break apart the Zitmo.apk file and analyze it and it's interactions with a desktop PC. Similar safety precautions were taken but because this was done on the

Eastern Michigan University campus in the Information Assurance lab, some additional steps were required.

As soon as the Zitmo.apk file was downloaded, the virtual machine (VM) that hosted the file was moved to a "host only" network setting and the physical Ethernet cable was removed from the back of the computer. Should something have slipped past those two items, the work was done on the IA network in Roosevelt Hall, which means the investigation was done on a separate network from the main campus network. The investigation was also done on removable hard drives that were deep frozen, so once the physical machine was shut down, all files that had changed were reset to the default settings for that particular image.

While investigating the malware with REMnux, a Linux based operating system designed for malware analysis, and a Windows XP virtual machine, it was important to observe how opening the malware affected the system. This was accomplished with registration snapshot software called RegShot. RegShot took a quick snap shot of the registration keys before the malware was opened and then after, then reported on which registration keys were changed or added. This is important because you can quickly look at what the malware did to the registry which causes a lot of the headaches of malware as the system uses the registry to perform it's basic operations from starting up to shutting down and everything in-between. The other software that was used was the same software used in the forensics investigation was process monitor (ProcMon), and a network monitor like WireShark.

Analysis Discoveries and Results

The first discovery is that the Galaxy S2 is difficult to root. According to documentation on the Internet from various Android forum sites to root a Galaxy S2 you must not only flash it with a different Android OS, but also run different rooting toolkits. Most investigators and Android "rooters" reported that SuperOneClick was able to root the phone once it was hacked using the GingerBreak exploit in SuperOneClick. However in the lab this turned out to be false. Every exploit SuperOneClick offered with each version did not root the phone properly. After flashing the phone with what was reported as the correct flash PDA file, was unable to root the phone and ended up causing it to brick. To brick a phone means to make it inoperable and normally results in needing a new phone. I was able to flash it back to Ice Cream Sandwich version 4.0.4 and did not continue to attempt to root the phone. Further investigation into the case of rooting Android phones is suggested to fully understand their security vulnerabilities.

Even though the phone was not rooted and verified to be in a factory default mode, I was still able to inject and infect the phone within a matter of minutes. Because this was so easy it raised the question as to why. The answer is because in the Android operating system there is an option to "Allow downloads and instillation from third party app marketplaces." This meant I was able to directly inject the phone with this particular APK file and have it install without requiring the phone to be rooted. This raises further security vulnerabilities as to if this option is on or off by default, and if it is on, why.

The next things that were found came from reading a report written by Kindsight. Even though the Zitmo virus technically infected this phone, it required Zeus to be installed on a PC to be fully functional. Listed below are several screen shots of the

virus's GUI interface. The application is titled "Trusteer Rapport", which is the alias for the Zitmo virus.

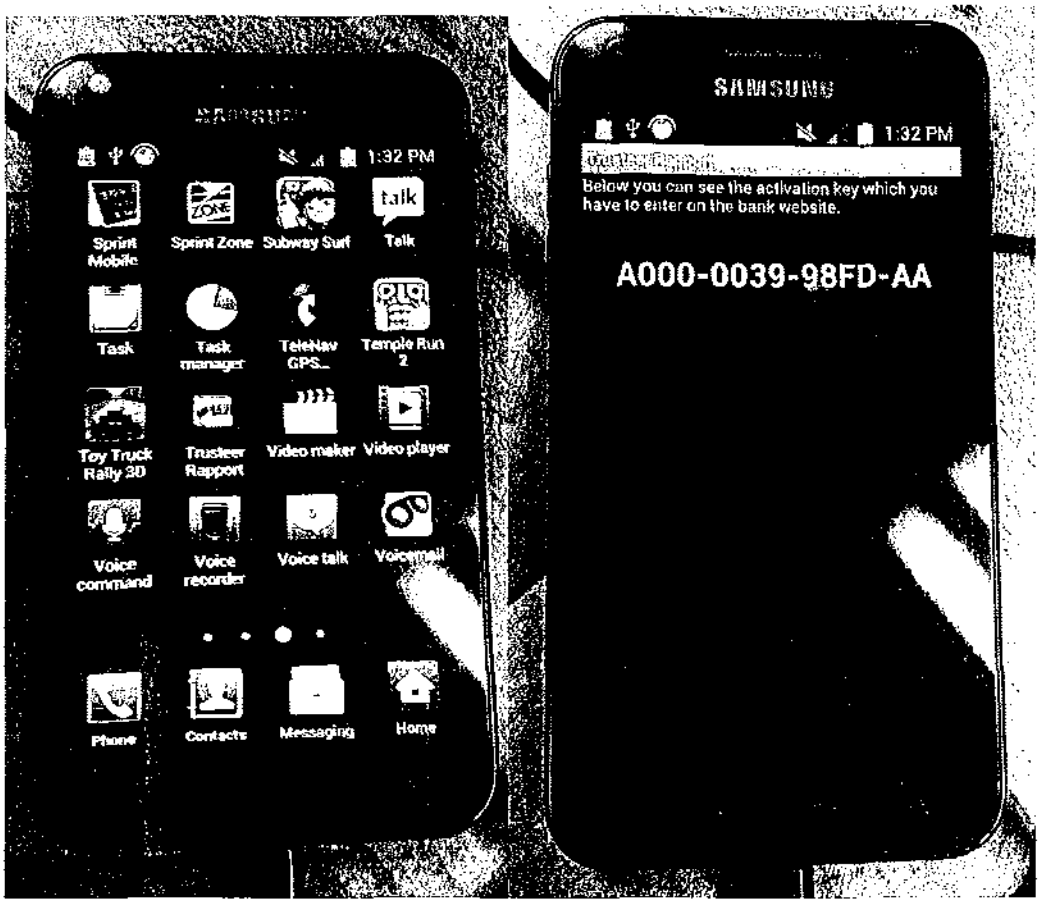

Figure 10: Zitmo Application "Trusteer Rapport" And "activation" information

From this investigation the Zitmo.apk installs the application called Trusteer Rapport which, when opened, gives the victim a unique ID that you enter into the "Trusteer Rapport" web application. It is safe to say that the website will not only infect your computer with the Zeus virus, but the UID that Zitmo displays on your phone connects your particular phone to this UID, allowing the attacker to use your personal information and anything you put into your phone / computer. It is almost like a syncing service between the Zitmo virus and the Zeus virus.

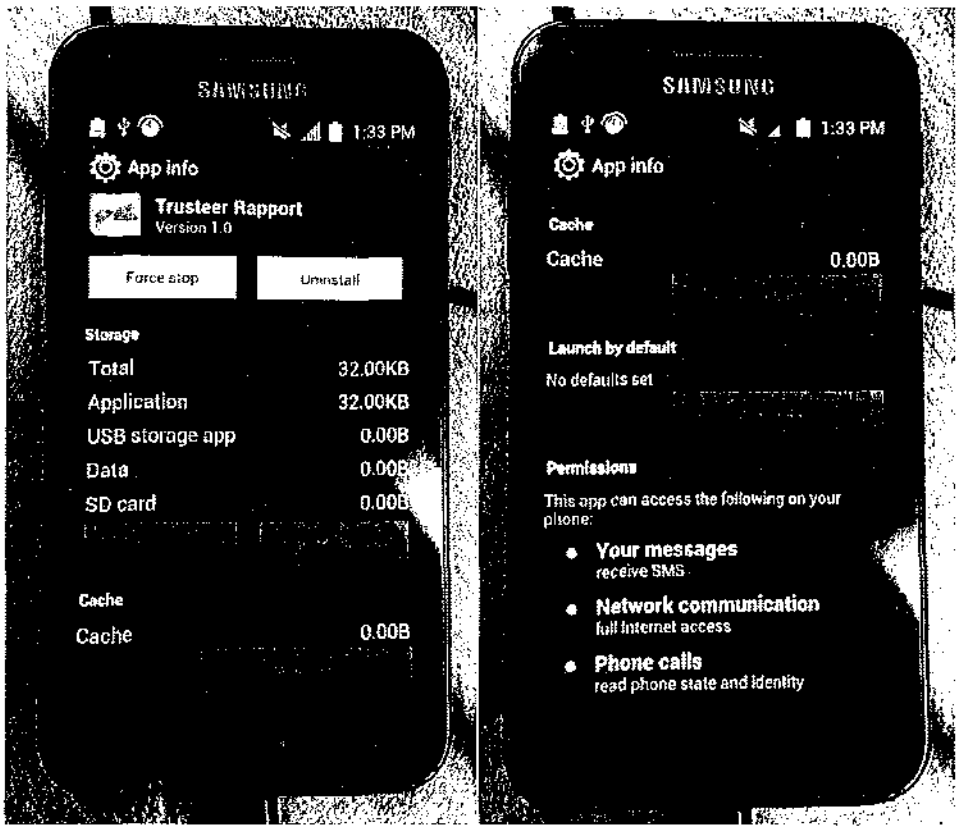

Figure 11: Application information for Trusteer Rapport.

When viewing the application in the App info section of the phone it doesn't look that different however when you take a look at the permission settings, this application can receive your SMS messages, has full Internet access, and can read your phone state and identity. For a banking application this raises red flags for several reasons. First off why does the banking application need access to SMS messages? If this was an application directly affiliated with a bank, like the Bank of America application, then at least it makes a little more sense. The application has permission to full Internet access, which means as long as it's connected to a network, 4G or Wi-Fi, means the application is going to do something. And finally no banking application needs access to your phone calls.

Conclusion

In conclusion, the current state of cell phone vulnerabilities leaves a wide gap in our security framework and puts all information at risk, especially if you are using an Android OS while downloading applications from third party sites. Even downloading some applications from the Google Play site has caused infections. To solve this issue, mobile phone companies and those that make the software used on these phones must work together on creating a more secure operating system. The other solution is the end-user must ensure they are using their phone safely and making sure that applications they download from the Internet are really what they say they are and safe.

References

Arthur, C. (2012, January 24). *The history of smartphones: timeline.* Retrieved November 21, 2013, from www.theguardian.com/technology/2012/jan/24/smartphones-timeline

Blue Coat. (2012). *BC_2013_Mobile_Malware_Report-v1d.pdf.* Retrieved November 24, 2013, from www.bluecoat.com/sites/default/files/documents/files/BC_2013_Mobile_Malware_Report-v1d.pdf

Chiang, H.-S., Lin, B., Shih, D.-H., & Shih, M.-H. (2008). Security aspects of mobile phone virus: a critical survey. *Indurstrial Management & Data Systems , 108* (4).

Cisco. (n.d.). *What Is The Difference: Viruses, Worms, Trojans, and Bots?* Retrieved November 12, 2013, from www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Cybercrime. (n.d.). *Collins English Dictionary – Complete & Unabridged 10th Edition.* Retrieved March 17 2014, from http://dictionary.reference.com/browse/cybercrime

Ewell, B. (2007, February 13). *VBS.Timofonica | Symantec.* Retrieved November 12, 2013, from www.symantec.com/security_response/writeup.jsp?docid=2000-121916-0443-99

F-Secure. (2013). *Mobile_Threat_Report_Q3_2013.* Retrieved November 24, 2013, from www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

Harvey, B. (1985). *What is a Hacker?* Retrieved October 22, 2013, from www.cs.berkeley.edu/~bh/hacker.html

Information Services & Technology. (n.d.). *Viruses, Spyware, and Malware | Information Services & Technology*. Retrieved October 27, 2013, from ist.mit.edu/security/malware

Keith, R. (2004). *How a Cell Phone Works.* Retrieved November 05, 2013, from http://iml.jou.ufl.edu/projects/fall04/keith/Works.htm

Kindsight. (2011, September). *Android_trojan_zitmo_final_pdf_17585.pdf.* Retrieved December 8, 2013 from http://www.kindsight.net/sites/default/files/android_trojan_zitmo_final_pdf_17585.pdf

Kindsight. (2010, September 14). *Attack in Depth: Zeus Banking Trojan | Kindsight.* Retrieved December 8, 2013, from http://www.kindsight.net/en/blog/2010/09/14/attack-in-depth-zeus-banking-trojan

Marshall Brian, J. L. (2000, November 14). *HowStuffWorks "3G Cell Phones".* Retrieved November 05, 2013, from http://electronics.howstuffworks.com/cell-phone9.htm

McAfee Labs. (2013). *rp-quarterly-threat-q2-2013.pdf.* Retrieved November 24, 2013, from www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf

Morphic. (n.d.). *Collins English Dictionary – Complete & Unabridged 10th Edition.* Retrieved October 23, 2013, from dictionary.reference.com/browse/morphic?s=t

Rouse, M. (2007, June). *What is cracker? Definitions from WhatIs.com.* Retrieved October 22, 2013, from http://searchsecurity.techtarget.com/definition/cracker

Shannon, H. (2007, February 13). *W32.Wullik.B@mm | Symantec.* Retrieved November 13, 2013, from www.symantec.com/security_response/writeup.jsp?docid=2003-110607-0328-99

Smith, M. (2011, January 5). *The 9 Types of Computer Viruses To Watch Out For & What They Do.* Retrieved October 2013, 2013, from www.makeuseof.com/tag/types-computer-viruses-watch/

Strickland, D. C. (2001, April 09). *HowStuffWorks "Network Protocols".* Retrieved November 05, 2013, from http://electronics.howstuffworks.com/smartphone3.htm

Wang, R. (2007, February 13). *SymbOS.Cardtrp.A | Symantec.* Retrieved November 13, 2013, from www.symantec.com/security_response/writeup.jsp?docid=2005-092215-2634-99

Virus. (n.d.). *Dictionary.com Unabridged.* Retrieved October 22, 2013, from Dictionary.com: dictionary.reference.com/browse/Virus?s=t