Prevalence of Malware in Mobiles, Causes and Prevention

Jaye Marvyn Agno
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
jragno@apc.edu.ph

Virgil joseph Cruz
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
vicruz@apc.edu.ph

Jose Francisco Canseco
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
jcanseco@apc.edu.ph

Jose Ricardo Milandro Hibaler
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
jthibaler@apc.edu.ph

Kenneth Bryan Lim
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
ealim@apc.edu.ph

Abstract
Prevalence of mobile utilization keeps on getting higher. It has in fact surpassed desktop and laptop PCs in terms of sales these past years. With this shift of interest of consumers in terms of communicating and doing tasks, Blackhat hackers are now also shifting their sights to these mobile gadgets. This is the reason why nowadays mobile gadgets such as smart phones and tablets are not exempted to malware infections and malicious attacks anymore.

This paper tackles about the prevalence of malware in mobile gadgets such as: 1.) Target platform for attacks and exploitations; 2.) Things that companies do to lessen mobile gadgets' security incidents. Moreover, it shows some latest statistics in terms of sales, most popular brand of smart phones and tablets and as well as the common means of attacking and infecting mobile gadgets.

Keywords: *mobile security, mobile malware, malware prevention, malware causes, mobile devices, smartphones, tablets*

II. Introduction

The field of IT is growing fast and evident in the past decades. One emerging technology is mobile. It is said that mobile gadget sales has surpassed the combined sales of both desktop and laptop PCs. As mobile solutions are being developed, threats are also being prevalent. Since 2011, mobile malwares became a big concern especially in Android devices. A 2013 research showed that Android devices attracted 98.05% of malware attacks. The threats includes Mobile Banking Trojans, Mobile Botnets, which was estimated to be 60% of malware threats, Backdoor.AndroidOs.Obad, which is probably the most versatile malware classified as of 2013, and many more. [10]

There are emerging ways to prevent the spread of mobile malwares, one of which is the increasing information drives that aims to increase the knowledge of the users with comes to mobile malware threats and its possible effects. Another one is keeping the mobile device software updated ensuring that the latest security functions are being updated constantly. [13]

A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. [11]

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a portmanteau of robot and network. [12]

III. Problem Statement

Since the use of mobile devices continue to grow together with its risks in getting infected, the researchers want to know the most attacked mobile platform in the market. This problem must be addressed in order for the people to be aware and be more cautious in using the platform. With this information, people will have the knowledge on how to secure their own mobile devices.

Another problem that the researchers want to solve is whether the security companies and other entities do anything to lessen the mobile platform's security incidents. Since attacks and exploitations continuously advance, they need to know whether those security companies are keeping up with the pace. They need to know if there are also new ways in protecting the attacked platform.

Lastly, the researchers want to determine the common ways on how the most targeted platform is attacked. This problem must be addressed in order for us to be aware how Blackhat hackers perform their attacks to the mobile devices. This information is needed so that these problems can be avoided and help the security companies in keeping the mobile platform more secure.

IV. Results and Discussion

According to Ashford's report that was published in November 2013, the threat of mobile malware has increased to 26% in the third quarter alone. It also stated that the mobile platform that is mostly attacked is the Android platform. It makes up 97% of the total threats while the remainder attacks the Symbian platform. This information is alarming since the Android platform shares a big percentage in the mobile market. It is estimated that the Android platform makes up about 79.3% of the total market share allowing Blackhat hackers to keep on concentrating their attacks to the said platform [1]. Because of this information, the researchers now need to know how Blackhat hackers perform their attacks and eventually determine possible solutions to this problem.

There are five (5) categories as to how the attacks are performed by Blackhat hackers: 1.) Malicious App; 2.) Cellular Network; 3.) Physical Access: Lost/Stolen Device; 4.) Physical Access: Reuse After Loss of Control; and 5.) Malicious Email/Web Page [2]. In July, a toolkit named Androrat APK binder has appeared [1]. What it does is it simplifies the insertion of malicious code into a legitimate Android application. Another growing form of attack is SMS-based attack coming from an already infected mobile device. What is does is it typically sends premium-rated SMS to generate profit illegally [1]. The following are some of the malware that hackers have used to attack the mobile platform.

In the year 2011, there are many issues regarding on the results of mobile malware. ADRD is one of them that issued commands to Android devices to send HTTP search requests to specific addresses. The malware increased site rankings for a specific website, resulting in additional advertising revenue. Another one is Droid KungFu which is a Trojan that sends sensitive information to an attacker and includes backdoor functionality that gave way to Droid KungFu 2 and Droid KungFu 3, which contained malware that confuse their communications and code making it much more difficult for security experts to identify and stop the malware. This malware is also encrypted that it cannot be easily detected by malware scanning engines. Droid Deluxe is another malware that can gain root access on its infected Android devices stole email credentials, social network account information and banking login information. It can bypass existing security controls. There was also a rise in fake installers. This malware tricks the users in paying via text messages or other free applications that sends their money to the developers of those fake installers [8].

Because of these recent developments in using malware, the researchers can say that the hackers are getting cleverer and are truly finding new ways to bypass any security measures that companies implement to protect their assets and clients. But not only private companies are trying to prevent or lessen attacks to the mobile platform but also some of the people who are in the academe. The researchers also found out that there are researches that try to improve the way they detect and prevent malware from spreading.

Based on the researches found, there are numerous ways of detecting mobile malware. There are those that are focused in the users network usage [3], [4]; there are also those that detect malware based on its behavior and signatures [5, 6]; and those that detect malware in a wider and more general manner [7].

V. Conclusion and Recommendation

Many incidents regarding mobile malwares in phones have popped up and have drastically increased through the years, mostly regarding android phones. Statistics show that malware attacks skyrocketed in 2012-2013[1]. The increase in users is one of the main reasons why mobile phones have become a major target in the eyes of cybercriminals. Most of the people now prefer to go mobile, and in order to prevent these malware attacks, we recommend the following:

1. **Regularly check your apps**. Check to see if there is anything suspicious in the apps you have downloaded. Anything suspicious should be deleted immediately. You can usually tell if malware is present if you notice decreased battery life (because there is something running in the background) or an increase in data use (as the malware transmits data from the phone). [9]

2. **Keep an eye on your bill**. Does anything look out of the ordinary? Also, contact your provider and block any unauthorized or unknown numbers. One of the most common fraud techniques criminals' use is sending SMS messages to premium-rate numbers using your phone. It means that for every SMS sent from your phone on the background, they are charging you a significant amount of money. [9]

3. **Install antivirus software**. Antivirus software is available to download for a reason. While not a guarantee, it could help minimize malware's overall effect on your phone. [9]

4. **Check phone settings**. Phone settings can be changed to prevent installation of content that isn't from trusted sources. Also, your phone should notify you before downloading any app to ensure you are restricted from unwanted activity. Make sure you auto-lock your phone and have a strong password in case it is lost or stolen. This can help keep your personal data private. Another good practice is disabling the "Wi-Fi auto connect" feature so your phone will only connect to previously known Wi-Fi networks. [9]

5. **Watch out for suspicious links**. Just like spam email, you have to be careful about following links sent from contacts within your address book. It is also very important to follow the same security advice to navigate the Internet using your phone, since you will be exposed to the same risks. Take into account that a malicious site that you browse can exploit a bug in your phone and install malware in the background. Be careful with sites that want you to install new software as well. [9]

6. **Download from trustworthy marketplaces only**. Apps should only be downloaded from trustworthy sources. The free ones, while attractive, could offer more than you bargained for. Take your time to read the reviews and the rating from other users to be sure the app is good for you before you download it. At the same time, even well-known stores like Google marketplace can fall prey to malicious apps. Security companies regularly find malicious apps in the marketplace. Case in point: Plankton was found embedded in several apparently benign apps. This kind of malicious app can send information to a remote server or receive and execute specified actions on your phone. [9]

References:

[1] Ashford, W. (2013, November). Mobile Malware Threats jump 26% in Third Quarter.TechTarget. [Online]. Available: http://www.computerweekly.com/news/2240208735/Mobile-malware-threats-jump-26-per-cent-in-third-quarter

[2] No Author. New Smartphones and the Risk Picture. NSA. [Online]. Available: http://www.nsa.gov/ia/_files/factsheets/mobilerisks.pdf

[3] Jin, R., Wang, B. Malware Detection for Mobile Devices Using Software-Defined Networking. [Online]. Available: http://nlab.engr.uconn.edu/papers/gree13.pdf

[4] Yen, T. F. (2011, August). Detecting Stealthy Malware Using Behavioral Features in Network Traffic. [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/staff/bios/tfyen/publications/Yen_Thesis.pdf

[5] Guo, D. F. A behavior analysis based Mobile Malware Defense System. [Online]. Available:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp&arnumber=6507944&queryText%3Dmobile+malware

[6] Patrui, A., et. al. (2013, May). Mobile malware visual analytics and similarities of Attack Toolkits (Malware gene analysis). [Online]. Available:

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp&arnumber=6567221&ranges%3D2012_2014_p_Publication_Year%26queryText%3Dmobile+malware
[7] Li, Y. Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp&arnumber=6381416&ranges%3D2012_2014_p_Publication_Year%26queryText%3Dmobile+malware
[8] No Author. 2011 Mobile Threats Reports. Juniper Networks.[Online]. Available: http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf
[9] No Author. Six Steps to Prevent Mobile Malware Attacks. IT Business Edge. [Online]. Available: http://www.itbusinessedge.com/slideshows/show.aspx?c=96079&slide=2
[10] No Author. (2013, December). Kaspersky Security Bulletin 2013: Overall Statistics for 2013. Kaspersky. [Online]. Available: http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013
[11] No Author. Trojan Horse. Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Trojan_horse_(computing)
[12] No Author. Botnet. Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Botnet
[13] No Author. 10 Tips to Prevent Mobile Malware. Sophos. [Online]. Available: http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/10-tips-to-prevent-mobile-malware.aspx